

PCI/JP 00/05742  
09/83039

REC'D 12 SEP 2000  
WIPO PCT

2000.06.30

日本国特許  
PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出願年月日  
Date of Application:

1999年 8月27日

JP 00/05742

CKJ

出願番号  
Application Number:

平成11年特許願第242295号

出願人  
Applicant(s):

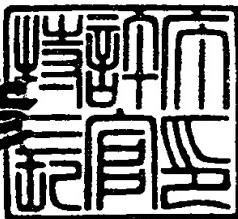
ソニー株式会社

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2000年 6月29日

特許庁長官  
Commissioner,  
Patent Office

近藤 隆彦



出証番号 出証特2000-3049727

【書類名】 特許願

【整理番号】 9900471602

【提出日】 平成11年 8月27日

【あて先】 特許庁長官 伊佐山 建志 殿

【国際特許分類】 H04L 12/16

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号ソニー株式会社内

【氏名】 石橋 義人

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100082740

【弁理士】

【氏名又は名称】 田辺 恵基

【手数料の表示】

【予納台帳番号】 048253

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9709125

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報配信システム及び情報受信装置

【特許請求の範囲】

【請求項1】

情報送信装置から情報受信装置に対して所定のコンテンツ鍵で暗号化されたコンテンツデータを配信する情報配信システムにおいて、

上記コンテンツの利用権を有する上記情報受信装置は、上記情報送信装置から配信される上記コンテンツデータを復号するための上記コンテンツ鍵を有し、上記コンテンツデータの利用権を持たない他の機器に対する再生コマンドを生成し、当該生成された再生コマンド及び上記コンテンツ鍵を上記他の機器に送信することにより、上記他の機器に上記コンテンツを再生させる  
ことを特徴とする情報配信システム。

【請求項2】

上記他の機器は、上記情報受信装置から上記コンテンツ鍵で暗号化された上記コンテンツデータを受け取り、当該受け取ったコンテンツデータを上記コンテンツ鍵及び上記再生コマンドを用いて再生する

ことを特徴とする請求項1に記載の情報配信システム。

【請求項3】

上記情報受信装置及び上記他の機器は、上記コンテンツの利用に際しての登録可否を表す登録情報を相互に検査し合い、当該検査結果が互いに利用可である場合に上記情報受信装置は上記他の機器に対して上記コンテンツ鍵及び上記再生コマンドを送信する

ことを特徴とする請求項1に記載の情報配信システム。

【請求項4】

情報送信装置から所定のコンテンツ鍵で暗号化されたコンテンツデータを受信する情報受信装置において、

上記コンテンツの利用権を有する場合に、上記情報送信装置から配信される上記コンテンツデータを復号するための上記コンテンツ鍵を有し、上記コンテンツデータの利用権を持たない他の機器に対する再生コマンドを生成し、当該生成さ

れた再生コマンド及び上記コンテンツ鍵を上記他の機器に送信することにより、  
上記他の機器に上記コンテンツを再生させる  
ことを特徴とする情報受信装置。

【請求項5】

上記他の機器の上記コンテンツの利用に際しての登録可否を表す登録情報を検査し、当該検査結果が利用可である場合に上記他の機器に対して上記コンテンツ鍵及び上記再生コマンドを送信する

ことを特徴とする請求項4に記載の情報受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報送信システムに関し、コンテンツ保有者又は販売者が、コンテンツを安全にコンテンツ利用者に配達し得る情報送信システムに適用して好適なものである。

【0002】

【従来の技術】

音楽などの情報（コンテンツ）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザがその情報処理装置でコンテンツを復号して、利用するシステムである。

【0003】

例えば図91に示すように、2つのコンテンツ送信装置および1つのコンテンツ受信装置が設けられている場合について説明する。

【0004】

第1のコンテンツ送信装置300は、データ暗号部301、データ暗号部302、コンテンツ鍵生成部303、耐タンパメモリ（Tamper Resistant Memory）304を有している。なお、ここで言う耐タンパメモリとは、第3者に容易にデータを読み出されなければならないものであればよく、特にハードウェア的制限は必要ない（例えば、入室管理された部屋の中にあるハードディスクや、パスワード管理されたパソコンのハードディスク等でよい）。耐タンパメモリ304にはコンテンツ

鍵 (Content Key)  $K_{co}$  を暗号化するのに必要な配送鍵 (Distribution Key)  $K_d$  が、予め電子配信サービスセンタ (図示せず) から供給され、保存されている。

## 【0005】

コンテンツ送信装置 300 は、コンテンツ受信装置 320 に渡すデータを生成するため、コンテンツ鍵生成部 303 を用いてコンテンツ鍵  $K_{co1}$  を生成し、この鍵を用いてデータ暗号部 301 にてコンテンツを暗号化する。また、コンテンツ鍵  $K_{co1}$  はデータ暗号部 302 にて配送鍵  $K_d$  を用いて暗号化される。これら暗号化されたコンテンツおよびコンテンツ鍵  $K_{co1}$  がコンテンツ受信装置 320 に送信される。

## 【0006】

因に、第2のコンテンツ送信装置 310 は、コンテンツ送信装置 300 と同様にして、データ暗号部 311、データ暗号部 312、コンテンツ鍵生成部 313、耐タンパメモリ 314 を有し、コンテンツ鍵生成部 313 においてコンテンツ鍵  $K_{co2}$  を生成し、この鍵を用いてデータ暗号部 311 によりコンテンツを暗号化する。またデータ暗号部 312 は電子配信サービスセンタ (図示せず) から供給される配送鍵  $K_d$  を用いてコンテンツ鍵  $K_{co2}$  を暗号化する。かくして第2のコンテンツ送信装置 310 は、暗号化されたコンテンツ及び暗号化されたコンテンツ鍵  $K_{co2}$  をコンテンツ受信装置 320 に送信する。

## 【0007】

コンテンツ受信装置 320 は、送受信部 321、上位コントローラ 322、暗号処理部 323、メモリ 324、データ復号部 325、データ復号部 326、耐タンパメモリ 327 を有する。なお、コンテンツ利用者が不特定多数であり、コンテンツ利用者が機器をどのように扱うか把握できないため、ここで言う耐タンパメモリとはハードウェア的に内部データが保護される必要性があり、従って暗号処理部 323 は、外部からアクセスしにくい構造を持った半導体チップで、多層構造を有し、その内部の耐タンパメモリはアルミニウム層等のダミー層に挟まれ、また、動作する電圧及び又は周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する。そして、耐タンパメモリ 327 には、電子配

信サービスセンタ（図示せず）から予め供給された配送鍵  $K_d$  が保存されている

#### 【0008】

因に、コンテンツ送信装置300及び310の耐タンパメモリ304、314は、外部からアクセス可能なメモリであるが、そのアクセス方法に制約を設けている。それがパスワードであったり、入室管理であったりする。一方、コンテンツ受信装置320の耐タンパメモリ327においては、メモリそのものが外部から不正にアクセスされない構造を有し、正規のアクセス手段で外部から内部データを読み出す方法も限定されているか、全くない。なお、耐タンパメモリ327は外部からその内部データを読み出すことは全くできないが、以前の鍵データ等を用いれば、外部からデータの変更のみできるアクセス方法がある場合がある。また、暗号処理部323内では、メモリにアクセスして所定のデータを読み出すことができるのに対して、外部から内部のメモリを読み出すことができないようになされている。

#### 【0009】

コンテンツ送信者300または310から送信されてきたコンテンツおよびコンテンツ鍵  $K_{co1}$  及び  $K_{co2}$  は、送受信部321で受信され、上位コントローラ322に引き渡される。上位コントローラ322は、これらのデータをいったんメモリ324に保存し、コンテンツを利用する場合には、コンテンツ鍵  $K_{co}$ 、コンテンツを暗号処理部323に引き渡す。これを受信した暗号処理部323は、データ復号部325で予め耐タンパメモリ327に保存しておいた配送鍵  $K_d$  を用いて復号化し、引き続きコンテンツをデータ復号部326でコンテンツ鍵  $K_{co}$  を用いて復号化し、コンテンツを利用する。この時、課金処理を伴う場合がある

#### 【0010】

##### 【発明が解決しようとする課題】

しかしながら、図91に示す従来の情報処理システムにおいては、コンテンツ送信装置300および310が同一の配送鍵  $K_d$  を使用しているため、互いにコンテンツ情報を盗み取ることができる問題があった。この問題点を解決するため

の一つの方法として、コンテンツ送信装置毎に異なる配送鍵 $K_d$ を使用することにより送信装置相互のコンテンツ情報の盗用を防止する方法が考えられる。ところが、この場合、コンテンツ受信装置が全ての配送鍵 $K_d$ を保持しておく必要があり、この分受信装置の構成及び受信方法が煩雑になる問題があった。

#### 【0011】

また、コンテンツを受信する情報受信装置のうち、コンテンツの利用権を有していない情報受信装置ではコンテンツを利用する事が困難であった。

#### 【0012】

##### 【課題を解決するための手段】

かかる課題を解決するため本発明においては、コンテンツの利用権を有する情報受信装置は、情報送信装置から配信されるコンテンツデータを復号するためのコンテンツ鍵を有し、コンテンツデータの利用権を持たない他の機器に対する再生コマンドを生成し、当該生成された再生コマンド及びコンテンツ鍵を他の機器に送信することにより、他の機器は受け取った再生コマンド及びコンテンツ鍵を用いてコンテンツを再生することができる。

#### 【0013】

##### 【発明の実施の形態】

以下、図面について本発明の一実施の形態を詳述する。

#### 【0014】

##### (1) 情報配信システム

図1は、本発明を適用したEMD(Electronic Music Distribution : 電子音楽配信)システム10を説明する図である。このシステムでユーザに配信されるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータで、この例の場合、1つのコンテンツは、1曲分の音楽データに相当する。コンテンツは、1つのコンテンツが1つの単位(シングル)として、または複数のコンテンツが1つの単位(アルバム)としてユーザに提供される。ユーザは、コンテンツを購入し(実際には、コンテンツ鍵 $K_{co}$ を利用する権利を購入し)、提供されるコンテンツを利用する(実際には、コンテンツ鍵 $K_{co}$ を用いてコンテンツを復号化し、利用する)。なお、勿論、音楽データだけでなく、映像、ゲームプログラ

ム等、コンテンツの販売全てに適用可能である。

【0015】

電子配信サービスセンタ（END Service Center）1は、コンテンツプロバイダ（Content Provider）2に個別鍵 $K_i$ 、コンテンツプロバイダ2の公開鍵証明書を送信し、サービスプロバイダ（Service Provider）3にサービスプロバイダ3の公開鍵証明書を送信し、ユーザホームネットワーク5に対しては配送鍵 $K_d$ や登録情報を送信し、ユーザホームネットワーク5から、コンテンツの利用に応じた課金情報等や登録情報を受信し、課金情報に基づいて利用料金を精算し、コンテンツプロバイダ2、サービスプロバイダ3および電子配信サービスセンタ1自身へ利益分配の処理を行う。

【0016】

コンテンツプロバイダ2は、デジタル化されたコンテンツを有し、自己のコンテンツであることを証明するために電子透かし（ウォーターマーク（Watermark））をコンテンツに挿入し、コンテンツを圧縮し、および暗号化し、コンテンツの取扱方針を生成し、署名データを付加してサービスプロバイダ3へ送信する。

【0017】

サービスプロバイダ3は、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク4を介して、コンテンツプロバイダ2から供給されたコンテンツに価格情報を追加し、署名データを付加して、ユーザホームネットワーク5に送信する。

【0018】

ユーザホームネットワーク5は、サービスプロバイダ3から価格情報を付して送付されたコンテンツ入手し、コンテンツ利用権を購入し、購入処理を実行する。購入した利用権は、例えば再生利用権であったり、コピーする権利であったりする。そして、購入処理により生成された課金情報は、ユーザの保持する機器の、暗号処理部内の耐タンパメモリに保存され、ユーザホームネットワーク5が配送鍵 $K_d$ を電子配信サービスセンタ1から入手する際に、電子配信サービスセンタ1に送信される。

## 【0019】

図2は、電子配信サービスセンタ1の機能の構成を示すブロック図である。サービスプロバイダ管理部11は、サービスプロバイダ3にサービスプロバイダ3の公開鍵証明書及び利益分配の情報を供給すると共に、必要に応じてコンテンツに付される情報（価格情報）を受信する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2に個別鍵 $K_i$ 、配送鍵 $K_d$ で暗号化した個別鍵 $K_i$ およびコンテンツプロバイダ2の公開鍵証明書を送信すると共に、利益分配の情報を供給し、必要に応じてコンテンツに付される情報（取扱方針）を受信する。著作権管理部13は、ユーザホームネットワーク5のコンテンツ利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) に送信する。鍵サーバ14は、システム全てに使用する鍵の生成、保持、管理を行っており、例えば、コンテンツプロバイダ毎に異なる個別鍵 $K_i$ が生成されるとともに、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ も併せて生成され、これらはコンテンツプロバイダ管理部12を介してコンテンツプロバイダ2に供給され、さらに配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ も必要に応じて認証局22に供給され、配送鍵 $K_d$ はユーザ管理部18を介してユーザホームネットワーク5に供給される。また、電子配信サービスセンタ1の公開鍵・秘密鍵、ユーザの保持する機器に固有の公開鍵・秘密鍵も全て生成、管理され、公開鍵は認証局22に送信され、公開鍵証明書作成に利用される。また、後述する暗号処理部92に固有の機器別IDに応じた保存鍵 $K_{save}$ を生成、保持する場合もある。

## 【0020】

電子配信サービスセンタ1からコンテンツプロバイダ2およびユーザホームネットワーク5を構成するホームサーバ51（後述する）への、鍵の定期的な送信の例について、図3乃至図6を参照に説明する。図3は、コンテンツプロバイダ2がコンテンツの提供を開始し、ユーザホームネットワーク5を構成するホームサーバ51がコンテンツの利用を開始する、2000年1月における、電子配信サービスセンタ1が有する配送鍵 $K_d$ 、個別鍵 $K_i$ 、コンテンツプロバイダ2が有する個別鍵 $K_i$ 、およびホームサーバ51が有する配送鍵 $K_d$ を示す図である

。なお、以下省略するが、コンテンツプロバイダ2は、個別鍵 $K_i$ に対応する、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ も保持しているものとする。

#### 【0021】

図3の例において、配送鍵 $K_d$ 、個別鍵 $K_i$ は、暦の月の初日から月の末日まで、使用可能であり、例えば、所定のビット数の乱数である”aaaaaaa”の値を有するバージョン1である配送鍵 $K_d$ 、”zzzzzzzz”の値を有するバージョン1である個別鍵 $K_i$ は、2000年1月1日から2000年1月31日まで使用可能（すなわち、2000年1月1日から2000年1月31日の期間にサービスプロバイダ3がユーザホームネットワーク5に配布するコンテンツを暗号化するコンテンツ鍵 $K_{co}$ は、バージョン1である個別鍵 $K_i$ で暗号化され、バージョン1である個別鍵 $K_i$ は、バージョン1である配送鍵 $K_d$ で暗号化されている）であり、所定のビット数の乱数である”bbbbbbb”の値を有するバージョン2である配送鍵 $K_d$ 、”yyyyyy”の値を有するバージョン2である個別鍵 $K_i$ は、2000年2月1日から2000年2月29日まで使用可能（すなわち、その期間にサービスプロバイダ3がユーザホームネットワーク5に配布するコンテンツを暗号化するコンテンツ鍵 $K_{co}$ は、バージョン2である個別鍵 $K_i$ で暗号化され、バージョン2である個別鍵 $K_i$ は、バージョン2である配送鍵 $K_d$ で暗号化されている）である。同様に、バージョン3である配送鍵 $K_d$ 、個別鍵 $K_i$ は2000年3月中に使用可能であり、バージョン4である配送鍵 $K_d$ 、個別鍵 $K_i$ は2000年4月中に使用可能であり、バージョン5である配送鍵 $K_d$ 、個別鍵 $K_i$ は2000年5月中に使用可能であり、バージョン6である配送鍵 $K_d$ 、個別鍵 $K_i$ は2000年6月中に使用可能である。

#### 【0022】

コンテンツプロバイダ2がコンテンツの提供を開始するのに先立ち、電子配信サービスセンター1は、コンテンツプロバイダ2に、2000年1月から6月まで利用可能な、バージョン1乃至バージョン6の6つの個別鍵 $K_i$ と、それぞれを同一バージョンの配送鍵 $K_d$ で暗号化したものを送信し、コンテンツプロバイダ2は、6つの個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を受信し、記憶する。6月分の個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を記

憶するのは、コンテンツプロバイダ2は、コンテンツを提供する前のコンテンツおよびコンテンツ鍵 $K_{c_0}$ の暗号化などの準備に、所定の期間が必要だからである。

#### 【0023】

また、ホームサーバ51がコンテンツの利用を開始するのに先立ち、電子配信サービスセンタ1は、ホームサーバ51に2000年1月から2000年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送鍵 $K_d$ を送信し、ホームサーバ51は、3つの配送鍵 $K_d$ を受信し、記憶する。3月分の配送鍵 $K_d$ を記憶するのは、ホームサーバ51が、回線の混雑等を原因として、電子配信サービスセンタ1に接続できないなどのトラブルにより、コンテンツの購入が可能な契約期間にもかかわらずコンテンツが購入できない等の事態を避けるためであり、また、電子配信サービスセンタ1への接続の頻度を低くしたり、個々の機器の電子配信サービスセンタ1への同時アクセスを押さえ、電子配信サービスセンタ1の負荷を低減するためである。

#### 【0024】

2000年1月1日から2000年1月31日の期間には、バージョン1である配送鍵 $K_d$ および個別鍵 $K_i$ が、電子配信サービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するホームサーバ51で利用される。

#### 【0025】

2000年2月1における、電子配信サービスセンタ1の配送鍵 $K_d$ および個別鍵 $K_i$ のコンテンツプロバイダ2、およびホームサーバ51への送信を図4で説明する。電子配信サービスセンタ1は、コンテンツプロバイダ2に、2000年2月から2000年7月まで利用可能な、バージョン2乃至バージョン7の6つの個別鍵 $K_i$ と、それぞれを同一バージョンの配送鍵 $K_d$ で暗号化したものを作成し、コンテンツプロバイダ2は、6つの個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を受信し、受信前に記憶していた個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ に上書きし、新たな個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を記憶する。電子配信サービスセンタ1は、ホームサー

バ51に2000年2月から2000年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送鍵 $K_d$ を送信し、ホームサーバ51は、3つの配送鍵 $K_d$ を受信し、受信前に記憶していた配送鍵 $K_d$ に上書きし、新たな配送鍵 $K_d$ を記憶する。電子配信サービスセンタ1は、バージョン1~7である配送鍵 $K_d$ および個別鍵 $K_i$ をそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送鍵 $K_d$ を利用できるようにするためである。

#### 【0026】

2000年2月1日から2000年2月29日の期間には、バージョン2である配送鍵 $K_d$ および個別鍵 $K_i$ が、電子配信サービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するホームサーバ51で利用される。

#### 【0027】

2000年3月1における、電子配信サービスセンタ1の配送鍵 $K_d$ および個別鍵 $K_i$ のコンテンツプロバイダ2、およびホームサーバ51への送信を図5で説明する。電子配信サービスセンタ1は、コンテンツプロバイダ2に、2000年3月から2000年8月まで利用可能な、バージョン3乃至バージョン8の6つの個別鍵 $K_i$ と、それぞれを同一バージョンの配送鍵 $K_d$ で暗号化したものを作成し、コンテンツプロバイダ2は、6つの個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を受信し、受信前に記憶していた個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ に上書きし、新たな個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を記憶する。電子配信サービスセンタ1は、ホームサーバ51に2000年3月から2000年5月まで、利用可能なバージョン3乃至バージョン5である3つの配送鍵 $K_d$ を送信し、ホームサーバ51は、3つの配送鍵 $K_d$ を受信し、受信前に記憶していた配送鍵 $K_d$ に上書きし、新たな配送鍵 $K_d$ を記憶する。電子配信サービスセンタ1は、バージョン1~8である配送鍵 $K_d$ および個別鍵 $K_i$ をそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送鍵 $K_d$ を利用できるようにするためである。

## 【0028】

2000年3月1日から2000年3月31日の期間には、バージョン3である配送鍵 $K_d$  および個別鍵 $K_i$  が、電子配信サービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するホームサーバ51で利用される。

## 【0029】

2000年4月1における、電子配信サービスセンタ1の配送鍵 $K_d$  および個別鍵 $K_i$  のコンテンツプロバイダ2、およびホームサーバ51への送信を図6で説明する。電子配信サービスセンタ1は、コンテンツプロバイダ2に、2000年4月から2000年9月まで利用可能な、バージョン4乃至バージョン9の6つの個別鍵 $K_i$  と、それを同一バージョンの配送鍵 $K_d$  で暗号化したものを作成し、コンテンツプロバイダ2は、6つの個別鍵 $K_i$  および配送鍵 $K_d$  で暗号化された個別鍵 $K_i$  を受信し、受信前に記憶していた個別鍵 $K_i$  および配送鍵 $K_d$  で暗号化された個別鍵 $K_i$  に上書きし、新たな個別鍵 $K_i$  および配送鍵 $K_d$  で暗号化された個別鍵 $K_i$  を記憶する。電子配信サービスセンタ1は、ホームサーバ51に2000年4月から2000年6月まで利用可能な、バージョン4乃至バージョン6である3つの配送鍵 $K_d$  を送信し、ホームサーバ51は、3つの配送鍵 $K_d$  を受信し、受信前に記憶していた配送鍵 $K_d$  に上書きし、新たな配送鍵 $K_d$  を記憶する。電子配信サービスセンタ1は、バージョン1～9である配送鍵 $K_d$  および個別鍵 $K_i$  をそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送鍵 $K_d$  を利用できるようにするためである。

## 【0030】

2000年4月1日から2000年4月30日の期間には、バージョン4である配送鍵 $K_d$  および個別鍵 $K_i$  が、電子配信サービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するホームサーバ51で利用される。

## 【0031】

このように、あらかじめ先の月の配送鍵 $K_d$  および個別鍵 $K_i$  を配布しておく

ことで、仮にユーザが1、2ヶ月全くセンタにアクセスしていないなくても、一応、コンテンツの買い取りが行え、時を見計らって、センタにアクセスすることにより鍵を受信することができる。

## 【0032】

電子配信サービスセンタ1の経歴データ管理部15(図2)は、ユーザ管理部18が集めたコンテンツの利用の実績を示す情報である課金情報、必要に応じてそのコンテンツに対応する価格情報(サービスプロバイダ3から送られてくるものと、ユーザが課金情報に付加して送ってくるものの、どちらか一方又は両方)、および必要に応じてそのコンテンツに対応する取扱方針(コンテンツプロバイダ2から送られてくるものと、ユーザが課金情報に付加して送ってくるものの、どちらか一方又は両方)を保持・管理し、サービスプロバイダ管理部11又はコンテンツプロバイダ管理部12等が課金情報や利用履歴等を利用する際にデータを出力する。なお、価格情報及び取扱方針は、課金情報に必要なデータが書き込まれている場合サービスプロバイダ3やコンテンツプロバイダ2から送られてこない場合がある。利益分配部16は、経歴データ管理部15から供給された、課金情報、必要に応じて価格情報、および取扱方針に基づき、電子配信サービスセンタ1、コンテンツプロバイダ2、およびサービスプロバイダ3の利益を算出する。これらの情報は、出納部20へ供給され、出納部20を介して利益分配を行う場合もあるが、利益分配を行なわず、これらの情報のみをサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、著作権管理部13に送信し、売上そのものはサービスプロバイダに入金させ、サービスプロバイダ3が各受益者に利益を分配する場合がある。相互認証部17は、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の所定の機器と後述する相互認証を実行する。

## 【0033】

ユーザ管理部18は、ユーザ登録データベースを有し、ユーザホームネットワーク5の機器から登録の要求があったとき、ユーザ登録データベースを検索し、その記録内容に応じて、その機器を登録したり、または登録を拒否する等の登録情報を作成する。ユーザホームネットワーク5が電子配信サービスセンタ1と接

続が可能な機能を有する複数の機器から構成されているとき、ユーザ管理部18は、登録情報に決済をする機器を規定し、決済IDを登録し、更に、コンテンツの購入処理動作を規定したり、ユーザホームネットワークを構成する機器の範囲を規定したり、取引停止等の情報を規定し、ユーザホームネットワーク5の所定の機器（決済可能機器）に送信する。

#### 【0034】

図7に示すユーザ登録データベースの例は、ユーザホームネットワーク5内で構築されたネットワークグループ毎の登録状況を示したもので、各グループには、グループのIDを示すグループID、ホームネットワーク5を構成する機器に固有のID、そのIDに対応して（すなわち、そのIDを有する機器毎に）、電子配信サービスセンタ1と接続が可能か否か、決済処理可能か否か、コンテンツの購入ができるか否か、決済処理を行うのはどの機器か、コンテンツの購入を依頼する機器はどれか、登録可能か否か、等の情報を記録する。

#### 【0035】

ユーザ登録データベースに記録されたグループIDはユーザホームネットワーク毎に割り振られ、このグループ単位で決済、情報更新が行われる。従って、原則的にはグループ内の代表機器が電子配信サービスセンタ1と通信、決済処理、情報更新を一括して行い、グループ内の他の機器は電子配信サービスセンタ1とのやりとりを直接は行わない。ユーザ登録データベースに記録されたIDは、機器毎に個別に割り振られたIDで、機器を識別するのに使用される。

#### 【0036】

ユーザ登録データベースに記録された電子配信サービスセンタ1と接続が可能か否かの情報は、その機器が、電子配信サービスセンタ1と物理的に接続が可能であるか否かを示し、接続できると記録された機器でも、決済処理可能であるとされた機器以外は、原則的に電子配信サービスセンタ1に接続されることがない（ただし、グループ内の代表機器が何らかの原因で決済処理動作しなくなった場合、代理で一時的に電子配信サービスセンタ1に接続されることがある）。また、接続ができないと記録された機器は、ユーザホームネットワーク5の決済処理可能な機器を介して、電子配信サービスセンタ1に、課金情報等を出力する。

【0037】

ユーザ登録データベースに記録された決済処理が可能か否かの情報は、その機器が、決済可能か否かを示す。ユーザホームネットワーク5が、コンテンツの利用権の購入などが可能な複数の機器で構成されているとき、その中の決済処理が可能である1台の機器は、電子配信サービスセンタ1に、ユーザホームネットワーク5の電子配信サービスセンタ1に登録されている全ての機器の、課金情報、必要に応じて価格情報、および取扱方針を送信し、決済処理の完了に応じて電子配信サービスセンタ1から配送鍵K<sub>d</sub>、登録情報を受信する。こうすることで、機器毎に処理を行うのに比べ、電子配信サービスセンタ1の処理が軽減される。

【0038】

ユーザ登録データベースに記録された購入処理が可能か否かの情報は、その機器が、コンテンツの利用権の購入ができるか否かを表す。購入不可の機器においては、他の購入可の機器から利用権の代理購入（別の機器で権利を購入し、その権利を全て譲り受けるものを言う。供給側には全く権利は残らない）、再配布（既に購入したコンテンツの利用権を、同一利用権内容または異なる利用権内容でもう一度購入し、別機器に供給する方式を言う。このとき、供給側には全く権利は残らない。再配布は、割引を行うことを主たる目的とする。割引の特典を受けられるのは、同一決済IDを使用しているグループであることが条件である。なぜなら、同一決済IDに属するグループ内の処理においては、電子配信サービスセンタ1の処理負担が軽減され、従って、その代償として割引が受けられるからである）または管理移動（コンテンツ再生権、特に無期限再生権の移動ができるが、再生権送信器においては再生権受信器がどの機器であるか管理され、再生権の返還がない場合、再度管理移動ができず、再生権受信器においては、再生権送信器がどの機器であるかが管理され、再度管理移動が全くできず、唯一、再生権を与えてくれた再生権送信器に再生権を返還することのみできる）を行ってもらってコンテンツ利用権を取得する。

【0039】

ここで、コンテンツの利用方法／利用権及び購入方法について簡単に説明する。コンテンツの利用方法としては、コンテンツの利用権を自己で管理保持してい

るもののが利用する場合と、他機器の保持する利用権を行使して自己の機器において利用する、2つのものがある。コンテンツの利用権としては、無制限再生権（コンテンツの再生期間及び回数に制限がないもの、なお、音楽コンテンツの場合は再生であるが、ゲームプログラム等では実行になる）、時間制限付き再生権（コンテンツの再生できる期間が限られているもの）、回数制限付き再生権（コンテンツの再生できる回数が限られているもの）、無制限複製権（コンテンツの複製期間及び回数に制限がないもの）、回数制限付き複製権（コンテンツの複製に回数制限があるもの）（複製権には、コピー管理情報なし複製権、コピー管理情報付き複製権（SCMS）等、その他専用メディア向け複製権等がある）（また時間制限付き複製権もある場合がある）、管理移動権がある。そして、利用権の購入方法としては、これらの利用権を直接購入する通常の購入に加え、既に購入した利用権の内容を別の内容に変更する利用権内容変更、他の機器で既に購入した権利に基づき利用権を別途購入する再配布、他の機器で利用権の購入を代理で行ってもらう代理購入、複数のコンテンツ利用権を一括して購入管理するアルバム購入等がある。

#### 【0040】

ユーザ登録データベースに記録された代理決済者に記された情報は、コンテンツの利用権を購入した際に生成した課金情報を、代理で電子配信サービスセンタ1に送信してもらう機器のIDを示す。

#### 【0041】

ユーザ登録データベースに記録された代理購入者に記された情報は、コンテンツの利用権の購入ができない機器に対し、代理で利用権の購入を行ってくれる機器のIDを示す。ただし、購入処理可能なグループ内機器全てが代理購入者ということにしておいた場合には、特に記録しておく必要はない。

#### 【0042】

ユーザ登録データベースに記録された登録が可能か否かの情報は、決済機関（例えば、銀行）、またはクレジットカード会社などから供給される料金の未払い、不正処理等の情報を基に、更新される。登録が不可と記録されたIDを有する機器の登録の要求に対して、ユーザ管理部18は、その登録を拒否し、登録を拒

否された機器は、以降、このシステムのコンテンツの購入ができないだけでなく、ユーザホームネットワーク5内の他機器とのデータ送受信もできなくなる。また場合によっては購入済のコンテンツの利用も制限される場合がある（ただし、電子配信サービスセンタ1等に機器を持ち込み、検査等を済ませた後再登録されることはある）。また、「登録可」、「登録不可」だけでなく、「決済未処理」、「一時停止」等の状態もあり得る。

#### 【0043】

また、ユーザ管理部18は、ユーザホームネットワーク5の機器から課金情報、登録情報、必要に応じて価格情報や取扱方針が供給され、課金情報、価格情報、および取扱方針を経歴データ管理部15に出力し、ユーザホームネットワーク5の機器に、配送鍵K<sub>d</sub>、登録情報を供給する。供給されるタイミングについては後述する。

#### 【0044】

ここで、図8を用いて登録情報を説明する。図8の登録情報はユーザ登録データベースの情報に加え、決済IDおよび署名が付加されており、同一決済グループの情報のみが含まれている。決済IDとは、決済を行う際に課金請求部19および出納部20が使用するユーザの、ユーザ情報データベース（例えば銀行口座番号やクレジットカード番号）内のIDを示している。署名の生成については、後述する。

#### 【0045】

再び図2にもどり、課金請求部19は、経歴データ管理部15から供給された、課金情報、必要に応じて価格情報、および取扱方針に基づき、ユーザへの課金を算出し、その結果を、出納部20に供給する。また、必要に応じてユーザ管理部18を介してユーザに決済情報を提供する。出納部20は、ユーザ、コンテンツプロバイダ2、およびサービスプロバイダ3への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決済処理を実行する。なお、出納部20は、サービスプロバイダ3へ売上のすべてを送金させ、利益分配部16を介して送信された分配金情報をもとに、サービスプロバイダ3が利益分配をする場合がある。監査部21は、ユーザホームネットワーク5の機器から供給された

課金情報、価格情報、および取扱方針を、コンテンツプロバイダ2から供給された取扱方針と、サービスプロバイダ3から供給された価格情報とからその正当性を監査する。

#### 【0046】

また、監査部21の処理としては、ユーザホームネットワーク5から入金された金額と、利益分配した合計金額又はサービスプロバイダ3へ送った金額との整合性を監査する処理や、ユーザホームネットワーク5の機器から供給された課金情報内のデータに例えば存在し得ないコンテンツプロバイダID、サービスプロバイダIDや考えられない取り分、価格等が含まれているか否かを監査する処理がある。

#### 【0047】

認証局22は、鍵サーバ14から供給された公開鍵の証明書を生成し、コンテンツプロバイダ2、サービスプロバイダ3へ供給し、ユーザ機器製造時にホームサーバ51の大容量記憶部68（後述する）や、据置機器52の小容量記憶部75（後述する）に保存される公開鍵証明書も生成する。コンテンツプロバイダ2がコンテンツのオーサリングを行わない場合、これを代替えする方法として、コンテンツを保持するコンテンツサーバ23、コンテンツオーサリング24がある。

#### 【0048】

図9は、コンテンツプロバイダ2の機能の構成を示すブロック図である。コンテンツサーバ31は、ユーザに供給するコンテンツを記憶し、電子透かし（ウォータマーク）付加部32に供給する。電子透かし付加部32は、コンテンツサーバ31から供給されたコンテンツに自分の所有物であることを示すコンテンツプロバイダIDを電子透かしの形で挿入し、圧縮部33に供給する。圧縮部33は、電子透かし付加部32から供給されたコンテンツを、ATRAC（Adaptive Transform Acoustic Coding）（商標）等の方式で圧縮し、コンテンツ暗号部34に供給する。因に、圧縮方式としてはATRACに代えてMP3やAAC等の方式を用いることができる。コンテンツ暗号部34は、圧縮部33で圧縮されたコンテンツを、コンテンツ鍵生成部35から供給された鍵（以下、この鍵をコンテ

ンツ鍵 $K_{co}$ と称する)を用いて、DES(Data Encryption Standard)などの共通鍵暗号方式で暗号化し、その結果を署名生成部38に出力する。

#### 【0049】

コンテンツ鍵生成部35は、コンテンツ鍵 $K_{co}$ となる所定のビット数の乱数を生成し、この中で弱鍵(例えば、 $K_{co} = 1E1E1E1E0E0E0E0E$ や $1EE01EE00EF00EF0$ など)と呼ばれる暗号化に不適なビット列を除いたものをコンテンツ暗号部34、コンテンツ鍵暗号部36に供給する。そのような不適なビット列がない暗号アルゴリズムを使用するときは、不適なビット列を除く処理は不要である。コンテンツ鍵暗号部36は、コンテンツ鍵 $K_{co}$ を電子配信サービスセンタ1から供給された個別鍵 $K_i$ を使用して、DESなどの共通鍵暗号方式で暗号化し、その結果を署名生成部38に出力する。因に、暗号化方式としては、DESに限らず、例えばRSA(Rivest, Shamir, Adleman)等の公開鍵暗号方式を用いるようにしても良い。

#### 【0050】

DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして処理する暗号方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分(データ攪拌部)と、データ攪拌部で使用する鍵(拡大鍵)を共通鍵から生成する部分(鍵処理部)からなる。DESの全てのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

#### 【0051】

まず、平文64ビットは、上位32ビットのH0、および下位32ビットのL0に分割される。鍵処理部から供給された48ビットの拡大鍵K1、および下位32ビットのL0を入力として、下位32ビットのL0を攪拌したF関数の出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則に入れ替える「転置」の2種類の基本変換から構成される。次に、上位32ビットのH0と、F関数の出力が排他的論理和され、その結果はL1とされる。L0は、H1とされる。

#### 【0052】

上位32ビットのH0および下位32ビットのL0を基に、以上の処理を16

回繰り返し、得られた上位32ビットのH16および下位32ビットのL16が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

#### 【0053】

なお、本実施の形態では共通鍵暗号としてDESを示したが、NTT（商標）が提案するFEAL（Fast Encryption Algorithm）、IDEA（International Data Encryption Algorithm）、E2や、米国次期暗号標準であるAES（Advanced Encryption Standard）など、いずれでもよい。

#### 【0054】

取扱方針生成部37は、コンテンツの取扱方針を生成し、暗号化されるコンテンツに対応して、取扱方針を署名生成部38に出力する。なお、取扱方針生成部37は、生成した取扱方針を図示せぬ通信手段を介して電子配信サービスセンタ1に供給する場合があり、そのデータは保持・管理されている。署名生成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K<sub>co</sub>、暗号化された個別鍵K<sub>i</sub>、取扱方針に電子署名を付加し、コンテンツプロバイダ2の証明書C<sub>c</sub><sub>p</sub>と共にサービスプロバイダ3に送信する（以降、暗号化されたコンテンツ、暗号化されたコンテンツ鍵K<sub>co</sub>、暗号化された個別鍵K<sub>i</sub>、取扱方針のそれぞれにコンテンツプロバイダ3の秘密鍵を使用して電子署名を付加したものを、コンテンツプロバイダセキュアコンテナと称する）。なお、個々のデータに署名を別々に付加するのではなく、データ全体に対して1つの署名を付けるようにしてもよい。

#### 【0055】

相互認証部39は、電子配信サービスセンタ1と相互認証し、また、必要に応じてサービスプロバイダ3へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ3と相互認証する。メモリ40Aは、コンテンツプロバイダ2が秘密裏に保持しなくてはならない個別鍵K<sub>i</sub>を保持するため、第3者に容易にデータを読み出されない耐タンパメモリが望ましいが、特にハードウェア的制限は必要ない（例えば、入室管理された部屋の中にあるハードディスクや、パスワード管理されたパソコンのハードディスク等でよい）。また、メモリ

40Bは、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 、コンテンツプロバイダ2の公開鍵証明書が保存されるだけであるため、通常の記憶装置等何でもよい（公開情報であるため、秘密にする必要がない）。なお、メモリ40A、40Bを一つにしてもかまわない。

#### 【0056】

署名は、データまたは後述する証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵を使用して作成される。

#### 【0057】

ハッシュ関数および署名について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、MD(Message Digest)4、MD5、SHA(Secure Hash Algorithm)-1などが用いられる。

#### 【0058】

データと署名を送信する送信装置（コンテンツプロバイダ2）の署名生成部38は、例えば、公開鍵暗号方式である楕円曲線暗号を用いて署名を生成する。この処理を、図10を用いて説明する（EC-DSA(Elliptic Curve Digital Signature Algorithm)、IEEE P1363/D3）。ステップS1で、Mをメッセージ、pを標数、a、bを楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、Gを楕円曲線上のベースポイント、rをGの位数、 $K_s$ を秘密鍵（ $0 < K_s < r$ ）とする。ステップS2で乱数uを $0 < u < r$ になるように乱数発生ユニットで生成する。ステップS3でベースポイントをu倍した座標を計算する。なお、楕円曲線上の加算、2倍算は次のように定義されている。

#### 【0059】

$P = (X_0, Y_0)$ 、 $Q = (X_1, Y_1)$ 、 $R = (X_2, Y_2) = P + Q$ とし  
、 $P \neq Q$ の時、

$$X_2 = \lambda^2 - X_0 - X_1$$

$$Y_2 = \lambda (X_0 - X_2) - Y_0$$

$$\lambda = (Y_1 - Y_0) / (X_1 - X_0)$$

P = Q の時、

$$X_2 = \lambda^2 - 2X_0$$

$$Y_2 = \lambda (X_0 - X_2) - Y_0$$

$$\lambda = (3X_0^2 + a) / 2Y_0$$

となり、これらを用いて点Gのu倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。G、2G、4G…を計算し、uを2進数展開して1が立っているところに対応する( $2^i$ )×Gを加算する(iはuのLSBから数えた時のビット位置)）。ステップS4でc =  $X_v \bmod r$ を計算し、ステップS5でこの値が0になるかどうか判定し、0でなければステップS6へと進み、メッセージMのハッシュ値を計算し、f = SHA-1(M)とする。次に、ステップS7において、d = [(f + cK<sub>s</sub>) / u] mod r を計算し、ステップS8でdが0であるかどうか判定する。dが0出なければ、cおよびdを署名データとする。仮に、rを160ビット長の長さであると仮定すると、署名データは320ビット長となる。

#### 【0060】

ステップS5において、cが0であった場合、ステップS2に戻って新たな乱数を生成し直す。同様に、ステップS8でdが0であった場合も、ステップS2に戻って乱数を生成し直す。

#### 【0061】

署名とデータを受信した受信装置（ユーザホームネットワーク5）は、例えば、公開鍵暗号方式である楕円曲線暗号を用いて署名を検証する。この処理を、図11を用いて説明する。（受信装置は）ステップS10で、Mをメッセージ、pを標数、a、bを楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、Gを楕円曲線上のベースポイント、rをGの位数、GおよびK<sub>s</sub> Gを公開鍵（ $0 < K_s < r$ ）とする。ステップS11で署名データcおよびdが $0 < c, d < r$ を満たすか検査する。これを満たしていた場合、ステップS12で、メッセージMのハ

ハッシュ値を計算し、 $f = \text{SHA-1}(M)$  とする。次に、ステップ S 13 で  $h = 1 / d \bmod r$  を計算し、ステップ S 14 で  $h_1 = f h$ 、 $h_2 = c h \bmod r$  を計算する。ステップ S 15において、既に計算した  $h_1$  および  $h_2$  を用い、 $P = (X_p, Y_p) = h_1 G + h_2 K_s G$  を計算する。署名検証者は、公開鍵  $G$  および  $K_s G$  を知っているので、ステップ S 3 と同様にこの計算ができる。そして、ステップ S 16 で  $P$  が無限遠点かどうか判定し、無限遠点でなければステップ S 17 に進む（実際には、無限遠点の判定はステップ S 15 でできてしまう。つまり、 $P = (X, Y), Q = (X, -Y)$  の加算を行うと、前述の  $\lambda$  が計算できず、 $R$  が無限遠点であることが判明している）。ステップ S 17 で  $X_p \bmod r$  を計算し、署名データ  $c$  と比較する。この値が一致していた場合、ステップ S 18 に進み、署名が正しいと判定する。

#### 【0062】

署名が正しいと判定された場合、受信データは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信装置から送信されたデータであることがわかる。

#### 【0063】

ステップ S 11において、署名データ  $c$  および  $d$  が  $0 < c, d < r$  を満たさなかった場合、ステップ S 19 に進む。また、ステップ S 16 において、 $P$  が無限遠点であった場合もステップ S 19 に進む。さらにまた、ステップ S 17 において、 $X_p \bmod r$  の値が、署名データ  $c$  と一致していなかった場合にもステップ S 19 に進む。ステップ S 19 において、署名が正しくないと判定する。

#### 【0064】

署名が正しくないと判定された場合、受信データは改竄されているか、公開鍵に対応した秘密鍵を保持する送信装置から送信されたデータではないことがわかる。

#### 【0065】

なお、本実施の形態では、ハッシュ関数として SHA-1 を使用したが、MD 4、MD 5 などいずれの関数を使用してもよい。また、署名の生成および検証は RSA 暗号を用いて行ってもよい (ANSI X9.31-1)。

## 【0066】

次に公開鍵暗号方式の暗号化・復号化について説明する。暗号化および復号化で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対して、公開鍵暗号方式は、暗号化に使用する鍵と復号化に使用する鍵が異なる。公開鍵暗号方式を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開してもよい鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

## 【0067】

公開鍵暗号方式の中で代表的な楕円曲線暗号化方法を説明する。図12において、ステップS20で、 $M_x$ 、 $M_y$ をメッセージ、 $p$ を標数、 $a$ 、 $b$ を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 $G$ を楕円曲線上のベースポイント、 $r$ を $G$ の位数、 $G$ および $K_s$ 、 $G$ を公開鍵（ $0 < K_s < r$ ）とする。ステップS21で乱数 $u$ を $0 < u < r$ になるように生成する。ステップS22で公開鍵 $K_s$ 、 $G$ を $u$ 倍した座標 $V$ を計算する。なお、楕円曲線上のスカラー倍は署名生成のところで説明した方法と同一のため、ここでは説明を省略する。ステップS23で、 $V$ のX座標を $M_x$ 倍して $p$ で剰余を求め $X_0$ とする。ステップS24で $V$ のY座標を $M_y$ 倍して $p$ で剰余を求め $Y_0$ とする。なお、メッセージの長さが $p$ のビット数より少ない場合、 $M_y$ は乱数を使い、復号部では $M_y$ を破棄するようとする。ステップS25において、 $uG$ を計算し、ステップS26で暗号文 $uG$ 、（ $X_0$ 、 $Y_0$ ）を得る。

## 【0068】

ここで公開鍵暗号方式の復号化について、図13を用いて説明する。ステップS30において、 $uG$ 、（ $X_0$ 、 $Y_0$ ）を暗号文データ、 $p$ を標数、 $a$ 、 $b$ を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 $G$ を楕円曲線上のベースポイント、 $r$ を $G$ の位数、 $K_s$ を秘密鍵（ $0 < K_s < r$ ）とする。ステップS31において、暗号データ $uG$ を秘密鍵 $K_s$ 倍する。ステップS32では、暗号データの内、（ $X_0$ 、 $Y_0$ ）のX座標を取り出し、 $X_1 = X_0 / X_v \text{ mod } p$ を計算する。ステップS33においては、 $Y_1 = Y_0 / Y_v \text{ mod } p$ を計算する。そして、ステップS34で $X_1$ を $M_x$ とし、 $Y_1$ を $M_y$ としてメッセージを取り出す。この時、 $M_y$ をメッセージにしていなかった場合、 $Y_1$ は破棄する。

## 【0069】

このように公開鍵暗号方式では、秘密鍵を  $K_s$  、公開鍵を  $G$  、  $K_s \cdot G$  とすることで、暗号化に使用する鍵と復号化に使用する鍵を、異なる鍵とすることができます。

## 【0070】

また、公開鍵暗号方式の他の例としては RSA 暗号 (Rivest, Shamir, Adleman) が知られている。

## 【0071】

図14は、サービスプロバイダ3の機能の構成を示すブロック図である。コンテンツサーバ41は、コンテンツプロバイダ2から供給された、コンテンツプロバイダ2の公開鍵証明書および暗号化されているコンテンツを記憶している。コンテンツプロバイダ2の公開鍵証明書は、証明書検査部42で、証明書内の署名が認証局22の公開鍵で検証され、検証に成功した場合、コンテンツプロバイダ2の公開鍵を署名検証部43に供給する。署名検証部43においては、コンテンツサーバ41に記憶されている取扱方針に対するコンテンツプロバイダ2の署名を、先ほど検証したコンテンツプロバイダ2の公開鍵を用いて検証し、検証に成功した場合、取扱方針を値付け部44に供給する。値付け部44においては、取扱方針から価格情報を作成し、署名生成部45に供給する。署名生成部45においては、図示せぬ耐タンパメモリ（コンテンツプロバイダ2内の40Aと同様）に保持されたサービスプロバイダ3の秘密鍵を用い、価格情報に対する署名を生成する（以降、コンテンツプロバイダセキュアコンテナおよび価格情報にサービスプロバイダ3の秘密鍵を用いて電子署名を付加したものを、サービスプロバイダセキュアコンテナと称する）。なお、価格情報に署名を付加するのではなく、コンテンツプロバイダセキュアコンテナと価格情報全体に対して1つの署名を生成するようにしてもよい。そして、サービスプロバイダセキュアコンテナ、コンテンツプロバイダ2の公開鍵証明書、サービスプロバイダ3の公開鍵証明書を、ネットワーク4（図1）を介してユーザホームネットワーク5へ供給する。相互認証部46は、電子配信サービスセンタ1と相互認証し、また、必要に応じてコンテンツプロバイダ、およびインターネット、ケーブル通信等を介し、可能であ

ればユーザホームネットワーク5と相互認証する。

### 【0072】

図15は、ユーザホームネットワーク5の構成を示すブロック図である。ホームサーバ51は、ネットワーク4を介して、サービスプロバイダ3からコンテンツを含んだセキュアコンテナを受信し、コンテンツの利用権を購入し、その権利行使してコンテンツの復号、伸張、再生、複製を行う。

### 【0073】

通信部61は、ネットワーク4を介してサービスプロバイダ3、または電子配信サービスセンタ1と通信し、所定の情報を受信し、または送信する。上位コントローラ62は、入力手段63からの信号を受信し、所定のメッセージ等を表示手段64に表示し、暗号処理部65を利用してコンテンツの利用権購入処理等を行い、伸張部66に大容量記憶部68から読み出した暗号化されたコンテンツを供給し、大容量記憶部68に暗号化されたコンテンツ等を記憶する。入力手段63は、リモートコントローラからの信号や入力ボタンからの入力データを上位コントローラ62に送信する。表示手段64は、液晶表示器のような表示デバイスで構成され、ユーザに指示を出したり、情報を表示したりする。入力手段63および表示手段64は、必要に応じてタッチパネル式液晶表示器などになり、一つにまとめられる場合がある。暗号処理部65は、サービスプロバイダ3、または電子配信サービスセンタ1若しくはその他の機器の暗号処理部と相互認証し、コンテンツ利用権を購入すると共に、所定のデータの暗号化／復号化を行い、コンテンツ鍵K<sub>co</sub>および使用許諾条件情報を保持する外部メモリを管理し、さらに配送鍵K<sub>d</sub>、課金情報等を記憶する。伸張部66は、暗号処理部65と相互認証してコンテンツ鍵K<sub>co</sub>を受信し、このコンテンツ鍵K<sub>co</sub>を用いて上位コントローラ62から供給された暗号化されたコンテンツを復号化し、ATRAC等の所定の方式で伸張し、さらに所定の電子透かしをコンテンツに挿入する。外部メモリ67は、フラッシュメモリ等の不揮発メモリやバックアップ電源付き揮発性メモリで構成され、保存鍵K<sub>save</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>および使用許諾条件情報を保存する。大容量記憶部68はHDDや光ディスク等の記憶デバイスで、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコン

テナ（暗号化されたコンテンツ、個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 、取扱方針、価格情報及びそれらの署名）、公開鍵証明書、登録情報等が保存されている。

## 【0074】

電子配信サービスセンタ1と相互認証し、コンテンツ利用権を購入すると共に課金情報を生成し、所定のデータの復号化／暗号化を行い、コンテンツ鍵 $K_{co}$ および使用許諾条件情報を保持する外部メモリを管理し、さらに配送鍵 $K_d$ 、課金情報等を記憶する暗号処理部65は、制御部91、記憶モジュール92、登録情報検査モジュール93、購入処理モジュール94、相互認証モジュール95、暗号／復号化モジュール96、および外部メモリ制御部97から構成される。この暗号処理部65は、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパ性）を有する。

## 【0075】

制御部91は、上位コントローラ62からのコマンドに応じて各モジュールを制御すると共に、各モジュールからの結果を上位コントローラ62に返送する。記憶モジュール92は、購入処理モジュール94から供給された課金情報、および配送鍵 $K_d$ 等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送鍵 $K_d$ 等のデータを供給する。登録情報検査モジュール93は、上位コントローラ62から供給された登録情報を検査し、ユーザホームネットワーク5内の他の機器と相互認証するか否か、課金情報の授受をすべきか否か、コンテンツの再配布等をすべきか否かの判断を行う。購入処理モジュール94は、サービスプロバイダ3から受信したセキュアコンテナに含まれる取扱方針および価格情報（並びに、場合によっては、既に保持している使用許諾条件情報）から、新たに使用許諾条件情報を生成して外部メモリ制御部97又は制御部91に出力し、課金情報を生成して記憶モジュール92に出力する。相互認証モジュール95は、電子配信サービスセンタ1、ホームネットワーク5内の他の機器の暗号処理部および伸張部66との相互認証を実行し、必要に応じて、一時鍵 $K_{temp}$ （セッシ

ヨン鍵) を生成し、暗号／復号化モジュール96に供給する。

### 【0076】

復号／暗号化モジュール96は、復号化ユニット111、暗号化ユニット112、乱数発生ユニット113、署名生成ユニット114、および署名検証ユニット115から構成される。復号化ユニット111は、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を復号化したり、個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ を復号化したり、一時鍵 $K_{temp}$ で暗号化された各種データを復号化したりする。暗号化ユニット112は、復号化されたコンテンツ鍵 $K_{co}$ を、記憶モジュール92に保持されている保存鍵 $K_{save}$ で暗号化し、制御部91を介して外部メモリ制御部97に出力したり、一時鍵 $K_{temp}$ で各種データを暗号化したりする。乱数発生ユニット113は、所定の桁数の乱数を発生し、相互認証モジュール95や署名生成ユニット114に供給する。署名生成ユニット114は、制御部91から供給されたメッセージのハッシュ値を計算し、乱数発生ユニット113から供給された乱数を用いて署名データを生成して制御部91に出力する。署名検証ユニット115は、制御部から供給されたメッセージおよび署名データから署名が正しいかどうか判定し、その結果を制御部91に出力する。なお、署名の生成／検証方法については図10、図11について上述した場合と同様である。

### 【0077】

外部メモリ制御部97は、外部メモリ67を制御してデータの読み書きを行い、外部メモリ内のデータが改竄されていないかどうかデータ検証を行う。図16は、外部メモリ制御部97の動作を説明するブロック図である。図16において、記憶モジュール92には、N個の改竄防止用ハッシュ値(Integrity Check Value)が保存されている。外部メモリ67は、Nブロックのデータ領域に分割されており、それぞれのデータ領域にはM組のコンテンツ鍵 $K_{co}$ および使用許諾条件情報が書き込めるようになっている。また、外部メモリ67には、自由に使用できるその他の領域も用意されている。改竄防止用ハッシュ値ICVは、それに対応する外部メモリ67内の全データに対するハッシュ値になっている。外部メモリの読み出し手順および書き込み手順については、フローチャートを用いて後述する。

## 【0078】

コンテンツを復号化し、伸張し、所定の電子透かしを付加する伸張部66（図15）は、相互認証モジュール101、鍵復号モジュール102、復号モジュール103、伸張モジュール104、電子透かし付加モジュール105、および記憶モジュール106から構成される。相互認証モジュール101は、暗号処理部65と相互認証し、一時鍵 $K_{temp}$ を鍵復号モジュール102に出力する。鍵復号モジュール102は、外部メモリ67から読み出され一時鍵 $K_{temp}$ で暗号化されているコンテンツ鍵 $K_{co}$ を一時鍵 $K_{temp}$ で復号化し、復号モジュール103に出力する。復号モジュール103は、大容量記憶部68に記録されたコンテンツをコンテンツ鍵 $K_{co}$ で復号化し、伸張モジュール104に出力する。伸張モジュール104は、復号化されたコンテンツを、更にATRAC等の方式で伸張し、電子透かし付加モジュール105に出力する。電子透かし付加モジュール105は、購入処理を行った暗号処理部の個別IDを電子透かし技術を用いてコンテンツに挿入し、他の機器や図示せぬスピーカに出力し、音楽を再生する。

## 【0079】

記憶モジュール106には、暗号処理部65との相互認証に必要な鍵データが保存されている。なお、伸張部66は、耐タンパ性を備えていることが望ましい。

## 【0080】

外部メモリ67は、購入処理モジュール94で権利購入した際に生成した使用許諾条件情報や保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_{co}$ を記憶している。大容量記憶部68は、サービスプロバイダ3から供給されたセキュアコンテナや公開鍵証明書、登録情報等を記録する。

## 【0081】

装着された光ディスク、半導体メモリ等の記録メディア80にサービスプロバイダ3から供給されたコンテンツを記録し、再生する据置機器52は、通信部71、上位コントローラ72、暗号処理部73、伸張部74、小容量記憶部75、記録再生部76、入力手段77、表示手段78、外部メモリ79、および記録メディア80から構成される。通信部71は通信部61と同じ機能を有し、その説

明は省略する。上位コントローラ72は上位コントローラ62と同じ機能を有し、その説明は省略する。暗号処理部73は暗号処理部65と同じ機能を有し、その説明は省略する。伸張部74は伸張部66と同じ機能を有し、その説明は省略する。小容量記憶部75は大容量記憶部68と同じ機能を有しているものの、コンテンツそのものは保存されず、公開鍵証明書や登録情報等が記憶されるだけである。記録再生部76は、光ディスク、半導体メモリ等の記録メディア80が装着され、その記録メディア80にコンテンツを記録し、読み出したコンテンツを伸張部に出力する。入力手段77は入力手段63と同じ機能を有し、その説明は省略する。表示手段78は表示手段64と同じ機能を有し、その説明は省略する。外部メモリ79は外部メモリ67と同じ機能を有し、その説明は省略する。記録メディア80は、例えばMD（Mini Disk：商標）や、電子配信専用記憶メディア（半導体メモリを用いたMemory Stick：商標）であったりする。

#### 【0082】

ユーザが携帯し、音楽を再生して楽しむための機器である携帯機器53は、通信部81、上位コントローラ82、暗号処理部83、伸張部84、および外部メモリ85から構成される。通信部81は通信部61と同じ機能を有し、その説明は省略する。上位コントローラ82は上位コントローラ62と同じ機能を有し、その説明は省略する。暗号処理部83は暗号処理部65と同じ機能を有し、その説明は省略する。伸張部84は伸張部66と同じ機能を有し、その説明は省略する。外部メモリ85は外部メモリ67と同じ機能を有し、その説明は省略する。ただし、これらのメモリは半導体メモリだけとは限らず、HDD、書き換え可能な光ディスク等いずれでもよい。

#### 【0083】

図17は、電子配信専用の記録メディアの構成図を示したものである。電子配信されたコンテンツを保存する記録メディア120は、通信部121、暗号処理部122、および外部メモリ123から構成される。通信部121は、据置機器52（図15）の記録再生部76とデータの送受信を行う。据置機器52と相互認証し、コンテンツ利用権を譲り受け、所定のデータの復号化／暗号化を行い、コンテンツ鍵K<sub>co</sub>および使用許諾条件情報等を保持する外部メモリを管理し、さ

らに保存鍵  $K_{\text{save}}$  等を記憶する暗号処理部 122 は、その構成は暗号処理部 65 と同じ機能を有し、その説明は省略する。外部メモリ 123 は、保存鍵  $K_{\text{save}}$  で暗号化されたコンテンツ鍵  $K_{\text{co}}$ 、コンテンツ鍵  $K_{\text{co}}$  で暗号化されたコンテンツ、コンテンツの使用条件を定めた使用許諾条件情報、必要に応じて取扱方針、および価格情報を記憶している。

#### 【0084】

電子配信専用記録メディア 120 は、据置機器 52 の時に説明した記録メディアとは使い方が異なっている。通常の記録メディア 80 は、ホームサーバ 51 の大容量記憶部 68 の代用品であるのに対し、電子配信専用メディア 120 は、伸張部を持たない携帯機器に異なる。従って、コンテンツの再生を行う際には、伸張部 74 をもつ据置機器 52 のような機器が必要であるが、コンテンツを譲り受けたり、コンテンツを管理したりする機能に関してはホームサーバ 51 や携帯機器 53 と同様な処理ができる。これらの違いにより、通常の記録メディアに記録されたコンテンツは、記録した機器以外では再生することができないものの、電子配信専用記録メディア 120 に記録されたコンテンツは、記録した機器以外の機器でも再生することができるようになる。すなわち、通常の記録メディアには、コンテンツ鍵  $K_{\text{co}}$  で暗号化されたコンテンツがあるだけなので、コンテンツ鍵  $K_{\text{co}}$  を持つ（記録した）機器以外では再生ができない。一方、電子配信専用記録メディア 120においては、コンテンツ鍵  $K_{\text{co}}$  で暗号化されたコンテンツだけでなく、コンテンツ鍵  $K_{\text{co}}$  も、電子配信専用記録メディア 120 個有の保存鍵  $K_{\text{save}}$  で暗号化されて保持されているため、他の機器で再生することが可能になる。

#### 【0085】

つまり暗号処理部 122 の相互認証モジュール 128 と据置機器 52 の暗号処理部 73 の図示せぬ相互認証モジュール間で相互認証を行った後、専用記録メディア固有の保存鍵  $K_{\text{save}3}$  でコンテンツ鍵  $K_{\text{co}}$  を復号化し、共有した一時鍵  $K_{\text{te}}$  でコンテンツ鍵  $K_{\text{co}}$  を暗号化し、暗号処理部 73 へ送信して再生する。

#### 【0086】

図 18 は、各機器内のデータ記憶状況を示すブロック図である。ホームサーバ

51において、暗号処理部65内の記憶モジュール92には、機器を特定するための個別ID（暗号処理部を特定するものと同一）、課金処理する際に使用する決済用ID（必要に応じて個別IDで代替えできるし、登録情報にあるので不要の場合もある）、機器毎に異なる秘密鍵、保存鍵K<sub>save</sub>、電子配信サービスセンタ1と相互認証する際に使用する電子配信サービスセンタ1の公開鍵（電子配信サービスセンタ1の公開鍵証明書があれば不要）、公開鍵証明書を検証するための認証局22の公開鍵、伸張部66と相互認証する際に使用する共通鍵が記憶されている。これらのデータは、機器製造時に予め記憶されるデータである。これに対し、電子配信サービスセンタ1から定期的に配布される配送鍵K<sub>d</sub>、購入処理の際に書き込まれる課金情報、外部メモリ67内に保持するコンテンツ鍵K<sub>co</sub>および使用許諾条件情報の改竄チェック用のハッシュ値は、機器を使用し始めてから記憶されるデータであり、これらのデータも記憶モジュール92に記憶されている。伸張部66内の記憶モジュール106には、伸張部を特定するための個別ID、暗号処理部65と相互認証する際に使用する共通鍵が、機器製造時に予め記憶される。なお、暗号処理部65と伸張部66を1対1に対応させるため、それぞれの記憶モジュールに互いのIDを持たせておいても良い（相互認証が共通鍵で行われているため、結果的には対応した暗号処理部、伸張部でしかやりとりができない。但し処理としては公開鍵暗号方式の相互認証であっても良い。このとき保存されている鍵は共通鍵ではなく、伸張部66固有の秘密鍵になる）。

#### 【0087】

外部メモリ67には、コンテンツの復号を行う際に使用する保存鍵K<sub>save</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>、そのコンテンツ鍵K<sub>co</sub>を利用する際の条件を示す使用許諾条件情報が記憶されている。また、大容量記憶部68には、記憶モジュール92内にある機器個別の秘密鍵に対応する公開鍵の証明書（機器の公開鍵証明書）、登録情報、コンテンツプロバイダセキュアコンテナ（コンテンツ鍵K<sub>co</sub>で暗号化されたコンテンツおよびその署名、個別鍵K<sub>i</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>およびその署名、配送鍵K<sub>d</sub>で暗号化された個別鍵K<sub>i</sub>およびその署名、取扱方針およびその署名）、サービスプロバイダセキュアコンテナ（価格情報およびその署名）、コンテンツプロバイダ2の公開鍵証明書、サービスプロバイ

ダ3の公開鍵証明書が記憶されている。

#### 【0088】

携帯機器53には、ホームサーバ51が保持する暗号処理部65と同一の暗号処理部83、外部メモリ67と同一の外部メモリ85が備えられている（内部データが同一のものは省略されている。例えば、伸張部）。しかし、その内部に保持されるデータは、図に示すように若干異なっている。暗号処理部83内の記憶モジュールの保持するデータは、機器を特定するための個別ID、機器毎に異なる秘密鍵、保存鍵K<sub>save</sub>、電子配信サービスセンタ1と相互認証する際に使用する、電子配信サービスセンタ1の公開鍵（ただし、ホームサーバ51に電子配信サービスセンタ1との手続きを全て代行してもらう場合は必要ない）、公開鍵証明書を検証するための認証局22の公開鍵、伸張部84と相互認証する際に使用する共通鍵が記憶されている。これらのデータは、機器製造時に予め記憶されるデータである。また、外部メモリ85内に保持するコンテンツ鍵K<sub>co</sub>および使用許諾条件情報の改竄チェック用のハッシュ値、必要に応じて決済用ID、配送鍵K<sub>d</sub>、登録情報（の一部）（購入処理をしない場合、決済用ID、配送鍵K<sub>d</sub>は不要ない）は、機器を使用し始めてから記憶されるデータであり、これらのデータも記憶されている（購入処理を行う場合、課金情報も記憶される）。外部メモリ85には、暗号処理部83内にある機器個別の秘密鍵に対応する公開鍵の証明書、コンテンツ鍵K<sub>co</sub>で暗号化されたコンテンツおよびその署名（この他に、必要に応じて個別鍵K<sub>i</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>およびその署名、配送鍵K<sub>d</sub>で暗号化された個別鍵K<sub>i</sub>およびその署名必要に応じて、取扱方針およびその署名、価格情報およびその署名も記憶される場合がある）、コンテンツを復号化する際に使用する保存鍵K<sub>save</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>、そのコンテンツを利用する際の条件を示す使用許諾条件情報が記憶されている。また、必要に応じてコンテンツプロバイダ2の公開鍵証明書、サービスプロバイダ3の公開鍵証明書も記憶されている。

#### 【0089】

据置機器52には、ホームサーバ51の構成に加え、記録メディア80が備えられている。記録メディアとしては、通常のMDやCD-Rの場合もあるし、電

子配信専用の記憶メディアである場合もある。前者の場合、記憶されるデータはコピー禁止信号を付加された、復号化されたコンテンツになるが、勿論、暗号化されたコンテンツを入れておいてもよい（保存鍵  $K_{\text{save}}$  で暗号化されたコンテンツ鍵  $K_{\text{co}}$  も併せて記憶しておいても良い。この時、再生できるのは記憶した機器のみになる。なぜなら、保存鍵  $K_{\text{save}}$  は機器毎に異なっているからである）。

#### 【0090】

また、記憶メディアとしては、図19が考えられる。電子配信専用記憶メディア120において、暗号処理部122内にある記憶モジュール125には、記録メディアの個別ID、記録メディア毎に異なる秘密鍵、この秘密鍵に対応する公開鍵の証明書（外部メモリ123に記録しておいても良い）、コンテンツ鍵  $K_{\text{co}}$  を暗号化するのに使用する保存鍵  $K_{\text{save}}$ （一般に、記憶メディア毎に異なる）、電子配信サービスセンタ1の公開鍵（センタとやりとりしない場合や外部メモリ123に電子配信サービスセンタ1の公開鍵証明書が有る場合には必要ない）、認証局の公開鍵、外部メモリ123の改竄を検査するためのハッシュ値、登録情報（の一部）が記憶されている。外部メモリ123には、コンテンツ鍵  $K_{\text{co}}$  で暗号化されたコンテンツ（およびその署名）、保存鍵  $K_{\text{save}}$  で暗号化されたコンテンツ鍵  $K_{\text{co}}$ 、使用許諾条件情報が記憶されており、必要に応じて取扱方針（およびその署名）、価格情報（およびその署名）、コンテンツプロバイダ2の公開鍵証明書、サービスプロバイダ3の公開鍵証明書が記憶されている。

#### 【0091】

図20、図21は、電子配信サービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信される情報を説明する図である。コンテンツプロバイダ2は、コンテンツプロバイダセキュアコンテナ（その詳細は後述する）にコンテンツプロバイダ2の公開鍵証明書（その詳細は後述する）を付して、サービスプロバイダ3に送信する。また、コンテンツプロバイダ2は、必要に応じて取扱方針およびその署名、コンテンツプロバイダ2の証明書を電子配信サービスセンタ1に送信する。

#### 【0092】

サービスプロバイダ3は、コンテンツプロバイダ2の公開鍵証明書を検証し、

コンテンツプロバイダ2の公開鍵を入手し、受信したコンテンツプロバイダセキュアコンテナの署名を検証する（取扱方針のみ署名検証する場合もある）。署名の検証に成功した後、コンテンツプロバイダセキュアコンテナから取扱方針を取り出し、これを基に価格情報を生成し、価格情報に署名を付けてサービスプロバイダセキュアコンテナとする（その詳細は後述する）。コンテンツプロバイダセキュアコンテナ、サービスプロバイダセキュアコンテナ、コンテンツプロバイダ2の公開鍵証明書、およびサービスプロバイダ3の公開鍵証明書（その詳細は後述する）をユーザホームネットワーク5に送信する。また、サービスプロバイダ3は、必要に応じて価格情報およびその署名、サービスプロバイダ3の公開鍵証明書を電子配信サービスセンタ1に送信する。

#### 【0093】

ユーザホームネットワーク5は、受信したセキュアコンテナを検証した後、セキュアコンテナの中に含まれる取扱方針および価格情報に基づいて購入処理を行い、課金情報を生成して暗号処理部内の記憶モジュールに保存し、使用許諾条件情報を生成し、コンテンツ鍵 $K_{co}$ を復号化して保存鍵 $K_{save}$ で再暗号化し、使用許諾条件情報を生成し、再暗号化されたコンテンツ鍵 $K_{co}$ を外部メモリ67に保存しておく。そして、使用許諾条件情報に沿って、コンテンツ鍵 $K_{co}$ を保存鍵 $K_{save}$ で復号化し、この鍵でコンテンツを復号化して利用する。課金情報は、所定のタイミングで一時鍵 $K_{temp}$ で暗号化され、署名が付され、必要に応じて取扱方針および価格情報と共に電子配信サービスセンタ1に送信される。

#### 【0094】

電子配信サービスセンタ1は、課金情報および価格情報を基に使用料金を算出し、また電子配信サービスセンタ1、コンテンツプロバイダ2、およびサービスプロバイダ3それぞれの利益を算出する。電子配信サービスセンタ1は、さらに、コンテンツプロバイダ2から受信した取扱方針、サービスプロバイダ3から受信した価格情報、必要に応じて取扱方針、並びにユーザホームネットワーク5から受信した取扱方針、価格情報を比較し、サービスプロバイダ3またはユーザホームネットワーク5で取扱方針の改竄または不正な価格の付加等の不正がなかつたか否か等の監視をする。

## 【0095】

更に、電子配信サービスセンタ1は、コンテンツプロバイダ2にコンテンツプロバイダの公開鍵証明書を送信し、サービスプロバイダ3にサービスプロバイダの公開鍵証明書を送信する。また、工場出荷時に、各機器に応じて作成した公開鍵証明書を各機器に埋め込むため、各機器の公開鍵証明書に関するデータを工場に引き渡す。

## 【0096】

図22は、コンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナ1Aは、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツおよびその署名、個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ およびその署名、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ およびその署名、取扱方針および署名を含む。署名は、それぞれのデータにハッシュ関数を適用して生成されたハッシュ値に、コンテンツプロバイダ2の秘密鍵 $K_{scp}$ を用いて生成されたデータである。なお、図22の場合は鍵データ（個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ ）に対してそれぞれ別々に署名を生成し付加するようにしたが、各鍵データ（個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ ）を1つにまとめて1つの署名を生成し付加するようにしても良い。このように常に一体で使用される鍵データを1つにまとめて1つの署名を付加することにより、署名の検証が1回で済む。

## 【0097】

図23は、コンテンツプロバイダセキュアコンテナの他の例を説明する図である。コンテンツプロバイダセキュアコンテナ1Bは、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツおよびその署名、個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ およびその署名、取扱方針および署名を含む。

## 【0098】

図24は、コンテンツプロバイダセキュアコンテナの他の例を説明する図である。コンテンツプロバイダセキュアコンテナ1Cは、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツ、個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 、取扱方針、および署名を含む。署名は、コンテンツ鍵

$K_{co}$ で暗号化されたコンテンツ、個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 、および取扱方針にハッシュ関数を適用して生成されたハッシュ値に、コンテンツプロバイダ2の秘密鍵 $K_{scp}$ を用いて生成されたデータである。

## 【0099】

図25は、コンテンツプロバイダセキュアコンテナの他の例を説明する図である。コンテンツプロバイダセキュアコンテナ1Dは、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツ、個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ 、取扱方針、および署名を含む。署名は、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツ、個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ 、および取扱方針にハッシュ関数を適用して生成されたハッシュ値に、コンテンツプロバイダ2の秘密鍵 $K_{scp}$ を用いて生成されたデータである。

## 【0100】

図26は、コンテンツプロバイダ2の公開鍵証明書を説明する図である。コンテンツプロバイダ2の公開鍵証明書2Aは、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ2の名前、コンテンツプロバイダ2の公開鍵 $K_{pcp}$ 、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ2の名前、並びにコンテンツプロバイダ2の公開鍵 $K_{pcp}$ にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵 $K_{sca}$ を用いて生成したデータである。

## 【0101】

図27は、コンテンツプロバイダ2の公開鍵証明書の他の例を説明する図である。コンテンツプロバイダ2の公開鍵証明書2Bは、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書

の有効期限、コンテンツプロバイダ2の名前、コンテンツプロバイダ2の公開鍵 $K_{pcp}$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ2の名前、コンテンツプロバイダ2の公開鍵 $K_{pcp}$ 、並びに配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵 $K_{sca}$ を用いて生成したデータである。

### 【0102】

図28は、コンテンツプロバイダ2の公開鍵証明書のまた別の例を説明する図である。コンテンツプロバイダ2の公開鍵証明書2Cは、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ2の名前、コンテンツプロバイダ2の公開鍵 $K_{pcp}$ 、個別鍵 $K_i$ の一部を配送鍵 $K_d$ で暗号化した、所定の種類のデータ、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ2の名前、コンテンツプロバイダ2の公開鍵 $K_{pcp}$ 、並びに個別鍵 $K_i$ の一部を配送鍵 $K_d$ で暗号化した、所定の種類のデータにハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵 $K_{sca}$ を用いて生成したデータである。

### 【0103】

図29は、サービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナ3Aは、価格情報および署名で構成されている。署名は、価格情報に対し必要に応じてハッシュ関数を適用して生成されたハッシュ値に、サービスプロバイダ3の秘密鍵 $K_{ssp}$ を用いて生成されたデータである。

## 【0104】

図30は、サービスプロバイダセキュアコンテナの他の例を説明する図である。サービスプロバイダセキュアコンテナ3Bは、コンテンツプロバイダセキュアコンテナ、価格情報、および署名を含む。署名は、コンテンツプロバイダセキュアコンテナ、および価格情報にハッシュ関数を適用して生成されたハッシュ値に、サービスプロバイダ3の秘密鍵 $K_{ssp}$ を用いて生成されたデータである。

## 【0105】

図31は、サービスプロバイダ3の公開鍵証明書を説明する図である。サービスプロバイダ3の公開鍵証明書4Aは、公開鍵証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、サービスプロバイダ3の名前、サービスプロバイダ3の公開鍵 $K_{psp}$ 、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、サービスプロバイダ3の名前、並びにサービスプロバイダ3の公開鍵 $K_{psp}$ にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵 $K_{sca}$ を用いて生成したデータである。

## 【0106】

図32は、User機器の公開鍵証明書を説明する図である。User機器の公開鍵証明書5Aは、公開鍵証明書のバージョン番号、認証局がUser機器（正確には暗号処理部（専用のICチップ））に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、User機器の名前、User機器の公開鍵 $K_{pu}$ 、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がUser機器に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、User機器の名前、並びにUser機器の公開鍵 $K_{pu}$ にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵 $K_{sca}$ を用いて生成したデータである。

**【0107】**

図33および図34は取扱方針のデータフォーマットを示すものであり、当該取扱方針はコンテンツプロバイダ2によりシングルコンテンツ毎、またアルバムコンテンツ毎に生成され、ユーザホームネットワーク5が購入可能な利用権の内容を示す。

**【0108】**

シングルコンテンツに対する取扱方針（図33）のデータには、データの種別、取扱方針の種類、取扱方針の有効期限、コンテンツのID、コンテンツプロバイダのID、取扱方針のID、取扱方針のバージョン、地域コード、使用可能機器条件、使用可能User条件、サービスプロバイダのID、世代管理情報、当該取扱方針が示す購入可能な利用権を含むルールの数、当該ルールの格納位置を示すアドレス情報、そのアドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

**【0109】**

そして、ルールは、利用権毎に整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータ、最低販売価格、コンテンツプロバイダの利益額、当該コンテンツプロバイダの利益率、データサイズ、送信情報から構成されている。

**【0110】**

また、アルバムコンテンツに対する取扱方針（図34）のデータには、データの種別、取扱方針の種類、取扱方針の有効期限、アルバムのID、取扱方針のバージョン、コンテンツプロバイダのID、取扱方針のID、地域コード、使用可能機器条件、使用可能User条件、サービスプロバイダのID、当該アルバムを構成するシングルコンテンツの取扱方針の数、そのシングルコンテンツの取扱方針の格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納されたシングルコンテンツの取扱方針のデータパケット、世代管理情報、当該取扱方針が示す購入可能な利用権を含むルールの数、当該ルールの格納位置を示すアドレス情報、そのアドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

【0111】

そして、ルールは、シングルコンテンツの取扱方針のルールと同様に、利用権毎に整理番号として付けられたルール番号、利用権内容番号、パラメータ、最低販売価格、コンテンツプロバイダの利益額、当該コンテンツプロバイダの利益率、データサイズ、送信情報から構成されている。

【0112】

これら取扱方針において、データの種別はそのデータが取扱方針のデータであることを示し、取扱方針の種類は当該取扱方針がシングル又はアルバムコンテンツのいずれの取扱方針であるかを示している。取扱方針の有効期限は当該取扱方針の使用期間をその期限の切れる日付、又は使用を開始した基準となる日から期限の切れる日までの日数などによって示している。コンテンツのIDおよびアルバムのIDは取扱方針が示す購入可能なシングルコンテンツおよびアルバムコンテンツを示し、コンテンツプロバイダのIDは、当該取扱方針を規定したコンテンツプロバイダ2のIDを示している。

【0113】

また、取扱方針のIDは当該取扱方針を識別するためのものであり、例えば、同一コンテンツに対して複数の取扱方針が設定された場合などに当該取扱方針を識別するために使用される。取扱方針のバージョンは使用期間に応じて改訂した取扱方針のその改訂情報を示している。従って、取扱方針はこれら取扱方針のIDおよび取扱方針のバージョンにより管理される。

【0114】

地域コードは取扱方針の使用可能な地域をコード化して示しており、当該地域コードには取扱方針の使用可能な地域を限定する特定の地域を示すコードと、当該取扱方針を全ての地域で使用可能にするコードを割り当てることができる。使用可能機器条件は取扱方針を利用し得る機器の条件を示し、使用可能User条件は取扱方針を利用し得るユーザの条件を示している。

【0115】

サービスプロバイダのIDは取扱方針を利用するサービスプロバイダ3のIDを示しており、当該サービスプロバイダのIDには取扱方針を使用し得るサービ

スプロバイダ3を限定する特定のサービスプロバイダ3のIDと、当該取扱方針を複数（全て）のサービスプロバイダで使用し得るようにするIDとがある。

#### 【0116】

さらに、世代管理情報はコンテンツの再購入可能な最大回数を示す。署名は取扱方針から当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

#### 【0117】

また、ルールにおいて、利用権内容番号は、利用権内容毎に付加された番号であり、パラメータは権利内容のパラメータを示す。最低販売価格は利用権内容に応じてシングルおよびアルバムコンテンツを販売する際の最低の販売価格を示し、コンテンツプロバイダの利益額および利益率はシングルコンテンツおよびアルバムコンテンツが購入されたときにコンテンツプロバイダ2が得ることのできる利益の金額および販売価格に対する利益率を示している。データサイズは送信情報のデータサイズを示し、当該送信情報は、コンテンツプロバイダ2が設定した、利用権の購入によりユーザに加算されるポイントや、当該ポイントに応じた利用権の割引額でなるマイル情報や、必要に応じてコンテンツプロバイダ2が設定した各種情報からなる。

#### 【0118】

ここで、アルバムコンテンツの取扱方針において、複数のルールは、当該アルバムの購入形態を示している。また、アルバムコンテンツの取扱方針に格納された複数のシングルコンテンツの取扱方針において、当該取扱方針に格納されたルールは、それぞれ対応するシングルコンテンツがアルバムのなかから、シングル曲として単独で購入し得る、又は対応するシングルコンテンツがアルバム曲としてのみ購入し得る（すなわち、アルバムとして、他のシングルコンテンツと共に一体化してしか購入し得ない）等のようにアルバム内におけるシングルコンテンツの購入形態を示している。

#### 【0119】

従って、アルバムコンテンツの取扱方針においては、当該取扱方針のルールに

基づいて、アルバムコンテンツを購入し、又はシングルコンテンツの取扱方針のルールに基づいて、シングルコンテンツをシングル曲として購入するように、アルバムコンテンツと、シングル曲として販売し得るシングルコンテンツとのいずれも選択して購入し得るように定義されている。

【0120】

また、アルバムコンテンツの取扱方針においては、全体に対して署名を付けたことにより、当該署名を検証するだけで、この取扱方針に格納したシングルコンテンツの取扱方針の署名をそれぞれ検証しなくてもこのアルバムコンテンツの取扱方針と共に、各シングルコンテンツの取扱方針に対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

【0121】

因みに、シングルおよびアルバムコンテンツの取扱方針には、必要に応じて、コンテンツに対する署名の検証を実行するか否かを示す署名の検証の有無を格納し得る。これは、コンテンツのデータ量が比較的多く、署名の検証に時間がかかるためであり、取扱方針にかかる署名の検証の有無の情報が格納された場合には、当該情報に従ってコンテンツの署名の検証を実行し、又は当該検証を実行しないようにする。

【0122】

また、アルバムコンテンツの取扱方針においては、当該アルバムを構成する複数のシングルコンテンツの取扱方針を格納しているものの、これら複数のシングルコンテンツの取扱方針を格納しなくても良い。

【0123】

さらに、シングルおよびアルバムコンテンツの取扱方針においては、コンテンツプロバイダの利益額および利益率を電子配信サービスセンタ1により一括管理しても良いため、図35および図36に示すように、これらコンテンツプロバイダの利益額および利益率を除いて構成しても良い。

【0124】

図37および図38は価格情報のデータフォーマットを示すものであり、当該価格情報はサービスプロバイダ3において、コンテンツプロバイダ2から与えら

れるシングルコンテンツの取扱方針毎、またアルバムコンテンツの取扱方針毎に生成され、シングルコンテンツおよびアルバムコンテンツの価格を示す。

#### 【0125】

シングルコンテンツに対する価格情報（図37）のデータには、データの種別、価格情報の種類、価格情報の有効期限、コンテンツのID、サービスプロバイダのID、価格情報のID、価格情報のバージョン、地域コード、使用可能機器条件、使用可能User条件、コンテンツプロバイダのID、当該価格情報が付加された取扱方針のID、当該価格情報が示す購入可能な利用権を含むルールの数、当該ルールの格納位置を示すアドレス情報、そのアドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

#### 【0126】

そして、ルールは利用権毎に整理番号として付けられたルール番号、サービスプロバイダの利益額、当該サービスプロバイダの利益率、価格、データサイズ、送信情報から構成されている。

#### 【0127】

また、アルバムコンテンツに対する価格情報（図38）のデータには、データの種別、価格情報の種類、価格情報の有効期限、アルバムのID、サービスプロバイダのID、価格情報のID、価格情報のバージョン、地域コード、使用可能機器条件、使用可能User条件、コンテンツプロバイダのID、当該価格情報が付加された取扱方針のID、当該アルバムを構成するシングルコンテンツの価格情報の数、そのシングルコンテンツの価格情報の格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納されたシングルコンテンツの価格情報のデータパケット、当該価格情報が示す購入可能な利用権を含むルールの数、そのルールの格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

#### 【0128】

そして、ルールは、シングルコンテンツに対する価格情報のルールと同様に、利用権毎に整理番号として付けられたルール番号、サービスプロバイダの利益額、当該サービスプロバイダの利益率、価格、データサイズ、送信情報から構成さ

れている。

#### 【0129】

これら価格情報において、データの種別はこのデータが価格情報のデータであることを示し、価格情報の種類は当該価格情報がシングルコンテンツ又はアルバムコンテンツのいずれの価格情報であるかを示している。価格情報の有効期限は当該価格情報の使用期間をその期限の切れる日付、又は使用開始の基準となる日から期限の切れる日までの日数などによって示している。コンテンツのIDおよびアルバムのIDは価格情報が示す購入可能なシングルコンテンツおよびアルバムコンテンツを示し、サービスプロバイダのIDは当該価格情報を作成したサービスプロバイダ3のIDを示している。

#### 【0130】

また、価格情報のIDは当該価格情報を識別するためのものであり、例えば、同一コンテンツに対して複数の価格情報が設定された場合などに当該価格情報を識別するために使用される。価格情報のバージョンは使用期間に応じて改訂された価格情報の改訂情報を示している。従って、価格情報はこれら価格情報のIDおよび価格情報のバージョンにより管理される。

#### 【0131】

地域コードは価格情報の使用可能な地域をコード化して示しており、当該地域コードには価格情報の使用可能な地域を限定する特定の地域を示すコードと、当該価格情報を全ての地域で使用可能にするコードを割り当てることができる。使用可能機器条件は価格情報を利用し得る機器の条件を示し、使用可能User条件は価格情報を利用し得るユーザの条件を示している。コンテンツプロバイダのIDは価格情報を付加した取扱方針を規定したコンテンツプロバイダ2のIDを示している。取扱方針のIDは価格情報を付加した取扱方針を識別するためのものである。

#### 【0132】

さらに、署名は価格情報から当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれて

いる。

#### 【0133】

また、ルールにおいて、ルール番号は対応する取扱方針が示すルールのルール番号をそのまま用いる。サービスプロバイダの利益額および利益率はシングルコンテンツおよびアルバムコンテンツが購入されたときにサービスプロバイダ3が得ることのできる利益の金額および価格に対する利益率を示し、価格はサービスプロバイダ3により利用権内容および対応する最低販売価格に基づいて設定されたシングルコンテンツおよびアルバムコンテンツの販売価格を示す。データサイズは送信情報のデータサイズを示し、当該送信情報は、サービスプロバイダ3が設定した、利用権の購入によりユーザに加算されるポイントや、当該ポイントに応じた利用権の割引額であるマイル情報や、必要に応じてサービスプロバイダ3が設定した各種情報からなる。

#### 【0134】

ここで、サービスプロバイダ3は、価格情報を生成する際、対応する取扱方針が示す購入可能な全ての利用権を当該価格情報が示す購入可能な利用権として設定することができると共に、当該取扱方針が示す購入可能な全ての利用権のうちから任意に選定した利用権を価格情報が示す購入可能な利用権として設定することもでき、コンテンツプロバイダ2が規定した利用権を選定し得る。

#### 【0135】

また、アルバムコンテンツの価格情報において、複数のルールは、アルバムの購入形態に応じた販売価格を規定している。また、アルバムコンテンツの価格情報に格納された複数のシングルコンテンツの価格情報のうち、シングル曲として販売し得るシングルコンテンツの価格情報のルールは、当該シングル曲として販売し得るシングルコンテンツの販売価格を規定している。

#### 【0136】

従って、アルバムコンテンツの価格情報においては、当該価格情報1つでアルバムの販売価格と、シングル曲として販売し得るシングルコンテンツの販売価格とを認識し得るようになされている。

【0137】

また、アルバムコンテンツの価格情報においては、全体に対して署名を付けたことにより、当該署名を検証するだけで、この価格情報に格納したシングルコンテンツの価格情報の署名をそれぞれ検証しなくともこのアルバムコンテンツの価格情報と共に、各シングルコンテンツの価格情報に対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

【0138】

因みに、シングルおよびアルバムの価格情報においては、図33および図34について上述した取扱方針と同様にコンテンツに対する署名の検証の有無を格納し得る。また、アルバムコンテンツの価格情報においては、当該アルバムを構成する複数のシングルコンテンツの価格情報を格納しているものの、これら複数のシングルコンテンツの価格情報を格納しなくても良い。

【0139】

さらに、シングルおよびアルバムコンテンツの価格情報においては、サービスプロバイダの利益額および利益率を電子配信サービスセンタ1により一括管理しても良いため、図39および図40に示すように、これらサービスプロバイダの利益額および利益率を除いて構成しても良い。

【0140】

図41は使用許諾条件情報のデータフォーマットを示すものであり、当該使用許諾条件情報はユーザホームネットワーク5内の機器において、ユーザがコンテンツを購入した際、当該購入したコンテンツの取扱方針に基づいて作成され、この取扱方針の示す利用権内容のうちのユーザが選択した利用権内容を示す。

【0141】

使用許諾条件情報のデータには、データの種別、使用許諾条件情報の種類、使用許諾条件情報の有効期限、コンテンツのID、アルバムのID、暗号処理部のID、ユーザのID、コンテンツプロバイダのID、取扱方針のID、取扱方針のバージョン、サービスプロバイダのID、価格情報のID、価格情報のバージョン、使用許諾条件情報のID、再生権（利用権）に整理番号として付けられたルール番号、利用権内容番号、再生残り回数、再生権の有効期限、複製権（利用

権)に整理番号として付けられたルール番号、利用権内容番号、複製の残り回数、世代管理情報、再生権を保有する暗号処理部のIDが格納されている。

#### 【0142】

使用許諾条件情報において、データの種別はこのデータが使用許諾条件情報のデータであることを示し、使用許諾条件情報の種類は当該使用許諾条件情報がシングルコンテンツ又はアルバムコンテンツのいずれの使用許諾条件情報であるかを示している。使用許諾条件情報の有効期限は当該使用許諾条件情報の使用期間をその期限の切れる日付、又は使用開始の基準となる日から期限の切れる日までの日数などによって示している。

#### 【0143】

コンテンツのIDには購入されたシングルコンテンツを示すIDが記述され、アルバムのIDにはアルバムが購入されたときのみ当該アルバムを示すIDが記述される。実際には、コンテンツがシングルとして購入された場合、コンテンツのIDのみに購入されたシングルコンテンツを示すIDが記述され、また、コンテンツがアルバムとして購入された場合には、コンテンツのIDに、アルバムを構成する全てのシングルコンテンツのIDが記述され、かつアルバムのIDに購入されたアルバムを示すIDが記述される。従って、このアルバムのIDをみれば、購入されたコンテンツがシングルであるか、又はアルバムであるかを容易に判断し得る。

#### 【0144】

暗号処理部のIDはコンテンツを購入処理したユーザホームネットワーク5内の機器の暗号処理部を示す。ユーザのIDはコンテンツを購入したユーザホームネットワーク5内の機器を複数のユーザが共有しているときに、当該機器を共有する複数のユーザを示している。

#### 【0145】

また、コンテンツプロバイダのIDは使用許諾条件情報を作成するために用いた取扱方針を規定したコンテンツプロバイダ2のIDを示し、取扱方針のIDは当該使用許諾条件情報を作成するために用いた取扱方針を示す。取扱方針のバージョンは使用許諾条件情報を作成するために用いた取扱方針の改訂情報を示して

いる。サービスプロバイダのIDは使用許諾条件情報を作成するために用いた価格情報を作成したサービスプロバイダ3のIDを示し、価格情報のIDは当該使用許諾条件情報を作成するために用いた価格情報を示す。価格情報のバージョンは使用許諾条件情報を作成するために用いた取扱方針の改訂情報を示している。

従って、これらコンテンツプロバイダのID、取扱方針のID、取扱方針のバージョン、サービスプロバイダのID、価格情報のIDおよび価格情報のバージョンにより、ユーザが購入したコンテンツを提供したコンテンツプロバイダ2又はサービスプロバイダ3を知り得るようになされている。

#### 【0146】

使用許諾条件情報のIDはコンテンツを購入したユーザホームネットワーク5内の機器の暗号処理部が付けるものであり、当該使用許諾条件情報を識別するために使用される。再生権のルール番号は利用権のうちの再生権に付けられた整理番号を示し、対応する取扱方針および価格情報が示すルールのルール番号をそのまま用いる。利用権内容は後述する再生権の内容を示す。再生残り回数は購入したコンテンツに対して予め設定された再生回数のうちの残りの再生回数を示し、再生権の有効期限は購入したコンテンツの対する再生可能期間をその期限の切れる日時などによって示している。

#### 【0147】

また、複製権のルール番号は利用権のうちの複製権に付けられた整理番号を示し、対応する取扱方針および価格情報が示すルールのルール番号をそのまま用いる。利用権内容は後述する複製権の内容を示す。複製残り回数は購入したコンテンツに対して予め設定された複製回数のうちの残りの複製回数を示す。

#### 【0148】

さらに、世代管理情報はコンテンツを再購入した際に当該コンテンツの再購入可能な残り回数を示す。再生権を保有する暗号処理部のIDは現時点において再生権を保有する暗号処理部を示しており、管理移動したときには再生権を保有する暗号処理部のIDが変更される。

#### 【0149】

因みに、使用許諾条件情報においては、複製権に対して有効期限を規定しても

良く、当該有効期限を規定した場合には購入したコンテンツの対する複製可能期間をその期限の切れる日時などによって示す。

【0150】

図42は課金情報を示すものであり、当該課金情報はユーザホームネットワーク5内の機器により、コンテンツの購入の際に、当該コンテンツに対応する取扱方針および価格情報に基づいて生成される。

【0151】

課金情報のデータには、データの種別、暗号処理部のID、ユーザのID、コンテンツのID、コンテンツプロバイダのID、取扱方針のID、取扱方針のバージョン、サービスプロバイダのID、価格情報のID、価格情報のバージョン、使用許諾条件情報のID、ルール番号、コンテンツプロバイダ2の利益額および利益率、サービスプロバイダの利益額および利益率、世代管理情報、コンテンツプロバイダの設定した送信情報のデータサイズ、そのコンテンツプロバイダの設定した送信情報、サービスプロバイダの設定した送信情報のデータサイズ、そのサービスプロバイダの設定した送信情報、供給元のIDが格納されている。

【0152】

課金情報において、データの種別は当該データが課金情報であることを示し、暗号処理部のIDは、コンテンツの購入処理を実行して当該課金情報を生成した機器の暗号処理部を示す。ユーザのIDはコンテンツを購入したユーザホームネットワーク5内の機器を複数のユーザが共有しているときに、当該機器を共有する複数のユーザを示し、コンテンツのIDは当該購入されたコンテンツ（シングルコンテンツ又はアルバムコンテンツ）を示す。

【0153】

また、コンテンツプロバイダのIDは購入処理に用いた取扱方針を規定したコンテンツプロバイダ2のID（この取扱方針に含まれるコンテンツプロバイダのID）を示し、取扱方針のIDは当該購入処理に用いた取扱方針を示す。取扱方針のバージョンは、購入処理に用いた取扱方針の改訂情報を示す。サービスプロバイダのIDは購入処理に用いた価格情報を作成したサービスプロバイダ3のID（この価格情報に含まれるサービスプロバイダのID）を示し、価格情報のID

IDは当該購入処理に用いた価格情報を示す。価格情報のバージョンは、購入処理に用いた価格情報の改訂情報を示す。

#### 【0154】

使用許諾条件情報のIDは購入処理の際に作成した使用許諾条件情報のIDを示し、ルール番号は購入された利用権に整理番号として付けられたルール番号を示す。コンテンツプロバイダの利益額および利益率はコンテンツの購入によりコンテンツプロバイダ2に分配される配当の金額および売上に対する割合を示し、サービスプロバイダの利益額および利益率は当該コンテンツの購入によりサービスプロバイダ3に分配される配当の金額および売上に対する割合を示す。

#### 【0155】

さらに、世代管理情報は購入されたコンテンツの世代を示す。また、コンテンツプロバイダの設定した送信情報のデータサイズおよびそのコンテンツプロバイダの設定した送信情報には、購入処理に用いた取扱方針が示すデータサイズと、送信情報をそのまま格納すると共に、サービスプロバイダの設定した送信情報のデータサイズおよびそのサービスプロバイダの設定した送信情報には購入処理に用いた価格情報が示すデータサイズと、送信情報をそのまま格納する。そして、供給元のIDは、購入処理したコンテンツの供給元の機器を示し、このIDはコンテンツの再購入が行われる毎に累積される。

#### 【0156】

因みに、課金情報においては、コンテンツプロバイダの利益額および利益率と、サービスプロバイダの利益額および利益率を電子配信サービスセンタ1により一括管理しても良いため、図43に示すように、これらコンテンツプロバイダの利益額および利益率およびサービスプロバイダの利益額および利益率を除いて構成しても良い。

#### 【0157】

図44は購入可能な利用権の内容を示したものであり、当該利用権としては、大きく分けて再生権、複製権、権利内容変更権、再購入権、追加購入権、管理移動権がある。

## 【0158】

再生権には、期間制限および回数制限のない無制限再生権と、再生期間を制限する期間制限付き再生権、再生の積算時間を制限する積算時間制限付き再生権、再生回数を制限する回数制限付き再生権がある。複製権には、期間制限、回数制限およびコピー管理情報（例えば、シリアルコピーマネージメント：SCMS）のないコピー管理情報なし無制限複製権、複製回数を制限するもののコピー管理情報のない回数制限付きおよびコピー管理情報なし複製権、期間制限および回数制限はないもののコピー管理情報を付加して提供するコピー管理情報付き複製権、複製回数を制限し、かつコピー管理情報を付加して提供する回数制限およびコピー管理情報付き複製権がある。因みに、複製権としては、この他に複製可能期間を制限する期間制限付き複製権（コピー管理情報を付加するものと、当該コピー管理情報を付加しないものとがある）や、複製の積算時間（すなわち、複製されたコンテンツの再生に要する積算時間）を制限する積算時間制限付き複製権（コピー管理情報を付加するものと、当該コピー管理情報を付加しないものとがある）等がある。

## 【0159】

また、権利内容変更権は上述したように既に購入した利用権の内容を別の内容に変更する権利であり、再購入権も上述したように他の機器で購入した権利に基づき利用権を別途購入する権利である。追加購入権は、既に単独で購入したコンテンツに当該コンテンツを含むアルバムの他のコンテンツを追加購入してアルバム化する権利であり、管理移動権は購入した利用権を移動して保有者を変更する権利である。

## 【0160】

次に、図33などに示されている利用権内容の具体例を説明する。実際に、無制限再生権のデータとしては、図45（A）に示すように、再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報が利用権内容の領域に格納される。期間制限付き再生権のデータとしては、図45（B）に示すように、再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日か

ら期限の切れる日までの日数などによって示す当該再生権の有効期限の情報が利用権内容の領域に格納される。

#### 【0161】

積算時間制限付き再生権のデータとしては、図45（C）に示すように再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報と、再生し得る積算時間の制限を示す日数および時間の情報とが利用権内容の領域に格納される。回数制限付き再生権のデータとしては、図45（D）に示すように、再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報と、再生し得る回数を示す再生回数の情報とが利用権内容の領域に格納される。

#### 【0162】

また、コピー管理情報なし無制限複製権のデータとしては、図45（E）に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報が利用権内容の領域に格納されている。回数制限付きおよびコピー管理情報なし複製権のデータとしては、図45（F）に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報と、複製し得る回数を示す複製回数の情報とが利用権内容の領域に格納される。

#### 【0163】

コピー管理情報付き複製権のデータとしては、図45（G）に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報が利用権内容の領域に格納されている。回数制限およびコピー管理情報付き複製権のデータとしては、図45（H）に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報と、複製し得る回数を示す複製回数の情報とが利用権内容の領域に格納される。

## 【0164】

さらに、権利内容変更権のデータとしては、図45（I）に示すように、当該権利内容変更権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該権利内容変更権の有効期限の情報と、変更前の利用権内容を検索するための旧ルール番号と、変更後の利用権内容を検索するための新ルール番号とが利用権内容の領域に格納される。因みに、利用権内容として、例えば、期間制限付き再生権1つをみても、その期間の設定により複数種類の期間制限付き再生権が存在するよう、利用権内容毎に複数種類の内容が存在する。従って、利用権内容を利用権内容番号だけでは管理し難いため、権利内容変更権においては、これら利用権内容毎の複数の内容毎に付けられたルール番号により利用権内容を管理する。

## 【0165】

再購入権のデータとしては、図45（J）に示すように、当該再購入権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再購入権の有効期限の情報と、再購入前の利用権内容を検索するための旧ルール番号と、再購入後の利用権内容を検索するための新ルール番号と、再購入し得る最大回数の示す最大配信世代情報とが利用権内容の領域に格納される。

## 【0166】

追加購入権のデータとしては、図45（K）に示すように、当該追加購入権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該追加購入権の有効期限の情報と、アルバムコンテンツを構成する複数のシングルコンテンツのうちの既に購入したシングルのコンテンツを示す最小保有コンテンツ番号および最大保有コンテンツ番号とが利用権内容の領域に格納される。

## 【0167】

管理移動権のデータとしては、図45（L）に示すように、当該管理移動権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該管理移動権の有効期限の情報が利用権

内容の領域に格納される。

#### 【0168】

因みに、かかる利用権内容として、例えば、ゲームのデータを複数のコンテンツに分割した際にこれらコンテンツを所定の順番に従って購入するためのコンテンツ購入権を規定しても良い。そして、コンテンツ購入権のデータとしては、図45(M)に示すように、当該コンテンツ購入権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該コンテンツ購入権の有効期限の情報と、既に購入されているコンテンツのIDと、既に購入された利用権内容を検索するための旧ルール番号と、新たに購入する利用権内容を検索するための新ルール番号とを利用権内容の領域に格納する。このようにすることで、連続したストーリーをもつゲームプログラムなどを、ユーザに連続して購入させるようにしたり、また、コンテンツ(ゲーム)そのものをアップグレードし得る。

#### 【0169】

図46はシングルコンテンツのデータフォーマットを示すものであり、当該シングルコンテンツのデータには、データの種別、コンテンツの種類、コンテンツの有効期限、コンテンツのカテゴリー、コンテンツのID、コンテンツプロバイダのID、コンテンツの暗号方式、暗号化したコンテンツのデータ長、その暗号化したコンテンツ、公開鍵証明書、署名が格納されている。

#### 【0170】

このシングルコンテンツにおいて、データの種別はそのデータがコンテンツのデータであることを示し、コンテンツの種類は当該コンテンツがシングルであることを示す。コンテンツの有効期限は当該コンテンツの配信期限をこの期限の切れる日付、又は配信を開始した基準となる日から期限の切れる日までの日数などによって示している。コンテンツのカテゴリーは当該コンテンツが音楽データ、プログラムデータ、映像データなどのいずれのカテゴリーのものであるかを示し、コンテンツのIDはこのシングルコンテンツを識別するためのものである。

#### 【0171】

コンテンツプロバイダのIDは、このシングルコンテンツを保有するコンテン

ツプロバイダ2のIDを示す。コンテンツの暗号方式は当該コンテンツの暗号に用いる暗号方式（例えば、DES）を示す。署名はシングルコンテンツのデータから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

#### 【0172】

また、図47はアルバムコンテンツのデータフォーマットを示すものであり、当該アルバムコンテンツのデータには、データの種別、コンテンツの種類、コンテンツの有効期限、アルバムのID、コンテンツプロバイダのID、シングルコンテンツの数、シングルコンテンツのアドレス情報、シングルコンテンツ、公開鍵証明書、署名が格納されている。

#### 【0173】

このアルバムコンテンツにおいて、データの種別はそのデータがコンテンツのデータであることを示し、コンテンツの種類は当該コンテンツがアルバムであることを示す。コンテンツの有効期限は当該コンテンツの配信期限をこの期限の切れる日付、又は配信を開始した基準となる日から期限の切れる日までの日数などによって示し、アルバムのIDはこのアルバムコンテンツを識別するためのものである。

#### 【0174】

コンテンツプロバイダのIDは、このアルバムコンテンツを保有するコンテンツプロバイダ2のIDを示す。シングルコンテンツの数はアルバムを構成するシングルコンテンツの数を示し、シングルコンテンツのアドレス情報は当該アルバムを構成するシングルコンテンツの格納位置を示し、そして、シングルコンテンツは当該アドレス情報の示す位置に実際に格納された、このアルバムを構成する複数のシングルコンテンツのデータパケットである。また、署名はアルバムコンテンツのデータから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

## 【0175】

そして、アルバムコンテンツにおいては、全体に対して署名を付けたことにより、当該署名を検証するだけで、このアルバムコンテンツに格納したシングルコンテンツの署名をそれぞれ検証しなくても当該アルバムコンテンツと共に、各シングルコンテンツに対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

## 【0176】

図4.8はシングルコンテンツ用の鍵のデータフォーマットを示すものであり、当該シングルコンテンツ用の鍵データには、データの種別、鍵データの種類、鍵の有効期限、コンテンツのID、コンテンツプロバイダのID、鍵のバージョン、コンテンツ鍵 $K_{co}$ の暗号方式、暗号化されたコンテンツ鍵 $K_{co}$ 、個別鍵 $K_i$ の暗号方式、暗号化された個別鍵 $K_i$ 、公開鍵証明書、署名が格納されている。

## 【0177】

シングルコンテンツ用の鍵データにおいて、データの種別はこのデータが鍵のデータであることを示し、鍵データの種類は当該鍵データがシングルコンテンツ用であることを示す。鍵の有効期限は鍵データに示す鍵（コンテンツ鍵 $K_{co}$ および個別鍵 $K_i$ ）の使用期間をその期限の切れる日付、又は鍵の使用を開始した基準となる日から期限の切れる日までの日数などによって示し、コンテンツのIDはコンテンツ鍵 $K_{co}$ により暗号化するシングルコンテンツを示す。コンテンツプロバイダのIDはコンテンツを保有し、かつコンテンツ鍵 $K_{co}$ を生成したコンテンツプロバイダ2のIDを示す。

## 【0178】

鍵のバージョンは使用期間に応じて改訂された鍵（コンテンツ鍵 $K_{co}$ および個別鍵 $K_i$ ）の改訂情報を示す。コンテンツ鍵 $K_{co}$ の暗号方式は個別鍵 $K_i$ を用いてコンテンツ鍵 $K_{co}$ を暗号化する際の暗号方式（例えば、DES）を示し、暗号化されたコンテンツ鍵 $K_{co}$ はその暗号方式により個別鍵 $K_i$ を用いて暗号化されたコンテンツ鍵 $K_{co}$ を示す。個別鍵 $K_i$ の暗号化方式は配送鍵 $K_d$ を用いて個別鍵 $K_i$ を暗号化する際の暗号方式（例えば、Triple-DES-CBC）を示し、暗号化された個別鍵 $K_i$ はその暗号方式により配送鍵 $K_d$ を用いて暗号化された個別鍵 $K_i$

を示す。署名はシングルコンテンツ用の鍵データから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

#### 【0179】

ここで、配送鍵 $K_d$  および個別鍵 $K_i$  はコンテンツプロバイダ2からシングルコンテンツ用の鍵データにより常に一体にされて配達される。そして、シングルコンテンツ用の鍵データにおいては、その全体に対して1つの署名が付加されている。従って、シングルコンテンツ用の鍵データを受け取った機器においては、暗号化されたコンテンツ鍵 $K_{co}$  および暗号化された個別鍵 $K_i$  に対してそれぞれ別々に署名を検証する必要がなく、シングルコンテンツ用の鍵データの1つの署名を検証するだけで当該暗号化されたコンテンツ鍵 $K_{co}$  および暗号化された個別鍵 $K_i$  に対する署名の検証をしたことになり、かくして、これら暗号化されたコンテンツ鍵 $K_{co}$  および暗号化された個別鍵 $K_i$  に対する署名の検証を簡易化し得る。

#### 【0180】

因みに、個別鍵 $K_i$  は、当該個別鍵 $K_i$  を用いてコンテンツ鍵 $K_{co}$  を暗号化するコンテンツプロバイダのIDと共に暗号化される。実際に、トリプルデスのCBCモードと呼ばれる暗号化方式によってコンテンツプロバイダのIDと共に個別鍵 $K_i$  を暗号化する方法を図49を用いて説明する。すなわち、かかる暗号化方式では、所定の初期値と、個別鍵 $K_i$  (64bit) とを接続した後、配送鍵 $K_d$  を用いてトリプルデスのCBCモードによる暗号化方式で暗号化し、この結果、得られた64bitの第1の値をコンテンツプロバイダのID (64bit) と接続した後、再び配送鍵 $K_d$  を用いてトリプルデスのCBCモードによる暗号化方式で暗号化し、かくして、64bitの第2の値を得る。そして、かかる暗号化方式では、第1の値と第2の値とを接続した16バイトのデータが、シングルコンテンツ用の鍵データに格納される暗号化された個別鍵 $K_i$  となる（この場合、第1の値はシングルコンテンツ用の鍵データに格納される暗号化された個別鍵 $K_i$  の始めの64bitのデータに相当し、また、第2の値は当該シングルコンテンツ用の鍵データ

に格納される暗号化された個別鍵 $K_i$  内の第1の値に続く64bit のデータとなる)。

#### 【0181】

また、図50はアルバムコンテンツ用の鍵データを示すものであり、当該アルバムコンテンツ用の鍵データには、データの種別、鍵データの種類、鍵の有効期限、アルバムのID、コンテンツプロバイダのID、鍵のバージョン、アルバムを構成するシングルコンテンツの暗号化の際に用いるシングルコンテンツ用の鍵データの数、その鍵データの格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納された鍵データパケット、公開鍵証明書、署名が格納されている。

#### 【0182】

アルバムコンテンツ用の鍵データにおいて、データの種別はこのデータが鍵のデータであることを示し、鍵データの種類は当該鍵データがアルバムコンテンツ用であることを示す。鍵の有効期限は鍵データに示す鍵（コンテンツ鍵 $K_{co}$ ）の使用期間をその期限の切れる日付、又は鍵の使用を開始した基準となる日から期限の切れる日までの日数などによって示し、アルバムのIDはコンテンツ鍵 $K_{co}$ により暗号化するシングルコンテンツからなるアルバムコンテンツを示す。コンテンツプロバイダのIDはアルバムコンテンツを暗号化するコンテンツプロバイダ2のIDを示す。

#### 【0183】

鍵のバージョンは使用期間に応じて改訂された鍵（コンテンツ鍵 $K_{co}$ ）の改訂情報を示す。署名はシングルコンテンツ用の鍵データから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

#### 【0184】

そして、アルバムコンテンツ用の鍵データにおいては、全体に対して署名を付けたことにより、当該署名を検証するだけで、当該アルバムコンテンツ用の鍵データに格納した複数のシングルコンテンツ用の鍵データの署名をそれぞれ検証し

なくても当該アルバムコンテンツ用の鍵データと共に、各シングルコンテンツ用の鍵データに対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

## 【0185】

図51は、1つの共通鍵で、共通鍵暗号であるDESを用いる、暗号処理部65と伸張部66との相互認証の動作を説明する図である。図51において、Aを伸張部66、Bを暗号処理部65とすると、暗号処理部65は64ビットの乱数 $R_B$ を生成し、 $R_B$ および自己のIDである $ID_B$ を、上位コントローラ62を介して伸張部66に送信する。これを受信した伸張部66は、新たに64ビットの乱数 $R_A$ を生成し、 $R_A$ 、 $R_B$ 、 $ID_B$ をDESのCBCモードで鍵 $K_{AB}$ を用いて暗号化し、上位コントローラ62を介して暗号処理部65に返送する。

## 【0186】

DESのCBCモードとは、暗号化する際に、一つ前の出力と入力を排他的論理和し、それから暗号化する手法である。本例で言うならば、

$$X = DES(K_{AB}, R_A + IV) \quad IV = \text{初期値} \quad + : \text{排他的論理和}$$

$$Y = DES(K_{AB}, R_B + X)$$

$$Z = DES(K_{AB}, ID_B + Y)$$

となり、出力は、X、Y、Zとなる。これらの式において、 $DES(K_{AB}, R_A + IV)$ は鍵 $K_{AB}$ を使ってデータ $R_A + IV$ をDESで暗号化することを表し、 $DES(K_{AB}, R_B + X)$ は鍵 $K_{AB}$ を使ってデータ $R_B + X$ をDESで暗号化することを表し、 $DES(K_{AB}, ID_B + Y)$ は鍵 $K_{AB}$ を使ってデータ $ID_B + Y$ をDESで暗号化することを表す。

## 【0187】

これを受信した暗号処理部65は、受信データを鍵 $K_{AB}$ で復号化し、 $R_B$ および $ID_B$ が、暗号処理部65が送信したものと一致するか検査する。この検査に通った場合、伸張部66を正当なものとして認証する。続けて、セッション鍵（一時鍵 $K_{temp}$ のこと、乱数により生成する） $SK_{AB}$ を生成し、 $R_B$ 、 $R_A$ 、 $SK_{AB}$ をDESのCBCモードで鍵 $K_{AB}$ を用いて暗号化し、上位コントローラ62を介して伸張部66に送信する。これを受信した伸張部66は、受信データを鍵 $K$

$R_B$  および  $R_A$  が、伸張部 6 6 が送信したものと一致するか検査する。この検査に通った場合、暗号処理部 6 5 を正当なものとして認証し、データ  $SK_{AB}$  をセッション鍵として以降の通信に使用する。なお、受信データの検査の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

### 【0188】

図 5 2 は、公開鍵暗号である、160ビット長の楕円曲線暗号を用いる、ホームサーバ 5 1 の暗号処理部 6 5 内の相互認証モジュール 9 5 と据置機器 5 2 の暗号処理部 7 3 内の図示せぬ相互認証モジュールとの相互認証の動作を説明する図である。図 5 2 において、A を暗号処理部 7 3 、B を暗号処理部 6 5 とすると、暗号処理部 6 5 は、64ビットの乱数  $R_B$  を生成し、上位コントローラ 6 2 、通信部 6 1 を介して据置機器 5 2 へ送信する。これを受信した据置機器 5 2 は、暗号処理部 7 3 において新たに 64 ビットの乱数  $R_A$  、および標数  $p$  より小さい乱数  $A_K$  を生成する。そして、ベースポイント G を  $A_K$  倍した点  $A_V$  を求め、 $R_A$  、 $R_B$  、 $A_V$  (X 座標と Y 座標) を連接し (64ビット + 64ビット + 160ビット + 160ビットで、448ビットになる) 、そのデータに対し、自己の持つ秘密鍵で署名データ A. Sig を生成する。なお、ベースポイントのスカラー倍は図 1 0 の署名の生成で説明した方法と同じであるためその説明は省略する。データの連接とは、例えば次のようになる。16ビットのデータ A と 16 ビットのデータ B を連接すると、上位 16 ビットのデータが A で、下位 16 ビットのデータが B になる 32 ビットのデータのことを言う。署名の生成は図 1 0 の署名の生成で説明した方法と同じであるためその説明は省略する。

### 【0189】

次に、暗号処理部 7 3 は、 $R_A$  、 $R_B$  、 $A_V$  および署名データ A. Sig を上位コントローラ 7 2 に引き渡し、上位コントローラ 7 2 は、据置機器 5 2 用の公開鍵証明書（小容量記憶部 7 5 に保存されている）を追加して通信部 7 1 を介してホームサーバ 5 1 に送信する。公開鍵証明書は図 3 2 で説明しているのでその詳細は省略する。これを受信したホームサーバ 5 1 は、暗号処理部 6 5 において据置機器 5 2 の公開鍵証明書の署名を検証する。署名の検証は、図 1 1 の署名の

検証で説明した方法と同じであるためその説明は省略する。次に、送られてきたデータのうち、乱数 $R_B$ が、暗号処理部65が送信したものと同一かどうか検査し、同一であった場合には署名データA. Sigを検証する。検証に成功したとき、暗号処理部65は暗号処理部73を認証する。なお、署名の検証は図11の署名の検証で説明した方法と同じであるためその説明は省略する。そして、暗号処理部65は、標数 $p$ より小さい乱数 $B_K$ を生成し、ベースポイントGを $B_K$ 倍した点 $B_V$ を求め、 $R_B$ 、 $R_A$ 、 $B_V$ (X座標とY座標)を連接し、そのデータに対し、自己の持つ秘密鍵で署名データB. Sigを生成する。最後に、暗号処理部65は、 $R_B$ 、 $R_A$ 、 $B_V$ および署名データB. Sigを上位コントローラ62に引き渡し、上位コントローラ62は、ホームサーバ51用の公開鍵証明書(大容量記憶部68に保存されている)を追加して通信部61を介して据置機器52に送信する。

#### 【0190】

これを受信した据置機器52は、暗号処理部73においてホームサーバ51の公開鍵証明書の署名を検証する。次に、送られてきたデータのうち、乱数 $R_A$ が、暗号処理部73が送信したものと同一かどうか検査し、同一であった場合には署名データB. Sigを検証する。検証に成功したとき、暗号処理部73は暗号処理部65を認証する。

#### 【0191】

両者が認証に成功した場合には、暗号処理部65は $B_K A_V$ ( $B_K$ は乱数だが、 $A_V$ は楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要)を計算し、暗号処理部73は $A_K B_V$ を計算し、これら点のX座標の下位64ビットをセッション鍵(一時鍵 $K_{temp}$ )として以降の通信に使用する(共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合)。因に、通信に使用するセッション鍵としては、X座標の下位64ビットに限らず、Y座標の下位64ビットを用いるようにしても良い。なお、相互認証後の秘密通信においては、データは一時鍵 $K_{temp}$ で暗号化されるだけでなく、その暗号化された送信データに署名が付されることがある。

## 【0192】

署名の検証、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

## 【0193】

図53は、ユーザホームネットワーク5内の決済可能機器が、電子配信サービスセンタ1へ課金情報を送信するときの動作を説明する図である。ユーザホームネットワーク5内の決済可能機器は、登録情報から代理決済すべき対象機器を検索し、相互認証を行い、課金情報を共有した一時鍵K<sub>temp</sub>（この鍵は、相互認証するたびに異なる）で暗号化して送らせる（このとき、データに署名が付いている）。全ての機器について処理が終わった後、電子配信サービスセンタ1と相互認証をし、共有した一時鍵で全ての課金情報を暗号化し、これらに署名データを付け、登録情報、必要に応じて取扱方針、価格情報と共に電子配信サービスセンタ1に送信する。なお、ユーザホームネットワーク5から電子配信サービスセンタ1へ送信される課金情報に、取扱方針のIDや価格情報のID等の金額の分配に必要な情報が含まれていることにより、情報量の多い取扱方針や価格情報は必ずしも送信する必要はない。ユーザ管理部18はこれを受信する。ユーザ管理部18は、受信した課金情報、登録情報、取扱方針、および価格情報に対する署名データの検証を行う。署名の検証は図11で説明した方法と同じなため詳細は省略する。次に、ユーザ管理部18は、相互認証のときに共有した一時鍵K<sub>temp</sub>で課金情報を復号化し、取扱方針、および価格情報と共に経歴データ管理部15に送信する。

## 【0194】

因みに、この実施の形態においては、相互認証後に送信されるデータは必要に応じて一時鍵K<sub>temp</sub>で暗号化される。例えばコンテンツ鍵K<sub>co</sub>や配送鍵K<sub>d</sub>は内容が見られてしまうとデータを不正に利用されてしまうため一時鍵K<sub>temp</sub>で暗号化して外部から見えないようにする必要がある。これに対して課金情報や使用許諾条件情報等は内容が見られても、データを不正に利用することができないため、必ずしも一時鍵K<sub>temp</sub>で暗号化する必要はないが、例えば課金情報の金額が改竄されたり使用許諾条件情報の使用条件が緩くなるように改竄されると金額の授

受に関係する当事者に損害が発生することになる。従って、課金情報や使用許諾条件情報には署名を付して送信することにより改竄を防止している。ただし、コンテンツ鍵  $K_{co}$  や配送鍵  $K_d$  を送信する場合にも署名を付けても良い。

#### 【0195】

そして、送信側では送られるデータに対して、又は送られるデータを一時鍵  $K_{temp}$  で暗号化したデータに対して署名を生成し、データ及び署名を送信する。受信側では、送られたデータが一時鍵  $K_{temp}$  で暗号化されていない場合には署名を検証することによりデータを得、又は送られたデータが一時鍵  $K_{temp}$  で暗号化されている場合には署名を検証した後に一時鍵  $K_{temp}$  でデータを復号することによりデータを得る。この実施の形態において、相互認証後に送信されるデータについては、以上 の方法により署名及び必要に応じて一時鍵  $K_{temp}$  による暗号化が施される場合がある。

#### 【0196】

ユーザ管理部18は、鍵サーバ14から配送鍵  $K_d$  を受信し、これを共有した一時鍵  $K_{temp}$  で暗号化して署名データを付加し、ユーザ登録データベースから登録情報を作成し、一時鍵  $K_{temp}$  で暗号化された配送鍵  $K_d$  、署名データ、登録情報をユーザホームネットワーク5内の決済可能機器に送信する。登録情報の作成方法については、図8で説明した通りでありここでの詳細説明は省略する。

#### 【0197】

課金請求部19は、決済を実行するとき、経歴データ管理部15から課金情報、必要に応じて取扱方針、および価格情報を受信し、ユーザへの請求金額を算出し、請求情報を出納部20に送信する。出納部20は、銀行等と通信し、決済処理を実行する。その際、ユーザの未払い料金等の情報があれば、それらの情報は決済報告の形で課金請求部19およびユーザ管理部18に送信され、ユーザ登録データベースに反映され、以降のユーザ登録処理、または決済処理時に参照される。

#### 【0198】

一時鍵  $K_{temp}$  で暗号化された配送鍵  $K_d$  、署名データ、登録情報を受信したユーザホームネットワーク5内の決済可能機器は、記憶してあった登録情報を更新

すると共に、登録情報を検査し、登録がなされていれば、署名データを検証した後、配送鍵  $K_d$  を一時鍵  $K_{temp}$  で復号化し、暗号処理部内の記憶モジュールに記憶されている配送鍵  $K_d$  を更新し、記憶モジュール内の課金情報を削除する。続いて、登録情報から代理決済すべき対象機器を検索し、当該検索により見つかった機器ごとに相互認証を行い、暗号処理部の記憶モジュールから読み出した配送鍵  $K_d$  を検索により見つかった機器ごとに異なる一時鍵  $K_{temp}$  で暗号化し、それぞれの機器ごとに署名を付け登録情報と共にそれぞれの機器に送信する。代理決済すべき対象機器が全て終わった時点で処理が終了する。

#### 【0199】

これらのデータを受信した対象機器は、決済可能機器と同様に登録情報を検査し、署名データを検証した後、配送鍵  $K_d$  を一時鍵  $K_{temp}$  で復号化し、記憶モジュール内の配送鍵  $K_d$  を更新し、課金情報を削除する。

#### 【0200】

なお、登録情報の登録項目が「登録不可」となっていた機器については、課金が行われなかったため、配送鍵  $K_d$  の更新、課金情報の削除は行わない（登録項目の内容は、使用を含めて一切の停止、購入処理の停止、処理が正常に行われた状態等、記述されていない種々の場合があり得る）。

#### 【0201】

図54は電子配信サービスセンタ1の利益分配処理の動作を説明する図である。経歴データ管理部15は、ユーザ管理部18から送信された課金情報、必要に応じて取扱方針、および価格情報を保持・管理する。利益分配部16は、経歴データ管理部15から送信された課金情報、必要に応じて取扱方針および価格情報からコンテンツプロバイダ2、サービスプロバイダ3、および電子配信サービスセンタ1それぞれの利益を算出し、その結果をサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、および出納部20に送信する。出納部20は、銀行等と通信し、決済を行う。サービスプロバイダ管理部11は、利益分配部16から受信した分配情報をサービスプロバイダ2に送信する。コンテンツプロバイダ管理部12は、利益分配部16から受信した分配情報をコンテンツプロバイダ3に送信する。

## 【0202】

監査部21は、経歴データ管理部15から課金情報、取扱方針、および価格情報を受信し、データに矛盾がないか監査する。例えば、課金情報内の価格が価格情報のデータと一致しているかどうか、分配率が一致しているかどうか等を監査し、取扱方針と価格情報が矛盾していないかどうか監査する。また、監査部21の処理としては、ユーザホームネットワーク5から入金された金額と、利益分配した合計金額又はサービスプロバイダ3へ送った金額との整合性を監査する処理や、ユーザホームネットワーク5の機器から供給された課金情報内のデータに例えば存在し得ないコンテンツプロバイダID、サービスプロバイダIDや考えられない取り分、価格等が含まれているか否かを監査する処理がある。

## 【0203】

図55は、電子配信サービスセンタ1の、コンテンツの利用実績をJASRACに送信する処理の動作を説明する図である。経歴データ管理部15は、ユーザのコンテンツの利用実績を示す課金情報を著作権管理部13および利益分配部16に送信する。利益分配部16は、課金情報からJASRACに対する請求金額および支払金額を算出し、支払情報を出納部20に送信する。出納部20は、銀行等と通信し、決済処理を実行する。著作権管理部13は、ユーザのコンテンツの利用実績をJASRACに送信する。

## 【0204】

次に、EMDシステムの処理について説明する。図56は、このシステムのコンテンツの配布および再生の処理を説明するフローチャートである。ステップS40において、電子配信サービスセンタ1のコンテンツプロバイダ管理部12は、コンテンツプロバイダ2に個別鍵K<sub>i</sub>、配送鍵K<sub>d</sub>で暗号化された個別鍵K<sub>i</sub>およびコンテンツプロバイダ2の公開鍵証明書を送信し、コンテンツプロバイダ2がこれを受信する。その処理の詳細は、図57のフローチャートを参照して後述する。ステップS41において、ユーザは、ユーザホームネットワーク5の機器（例えば、図15のホームサーバ51）を操作し、ユーザホームネットワーク5の機器を電子配信サービスセンタ1のユーザ管理部18に登録する。この登録処理の詳細は、図59のフローチャートを参照して後述する。ステップS42に

おいて、電子配信サービスセンタ1のユーザ管理部18は、ユーザホームネットワーク5と、図52について上述したように相互認証した後、ユーザホームネットワーク5の機器に、配送鍵 $K_d$ を送信する。ユーザホームネットワーク5はこの鍵を受信する。この処理の詳細は、図62のフローチャートを参照して説明する。

#### 【0205】

ステップS43において、コンテンツプロバイダ2の署名生成部38は、コンテンツプロバイダセキュアコンテナを生成し、それをサービスプロバイダ3に送信する。この処理の詳細は、図65のフローチャートを参照して後述する。ステップS44において、サービスプロバイダ3の署名生成部45は、サービスプロバイダセキュアコンテナを生成し、それをユーザホームネットワーク5へ、ネットワーク4を介して送信する。この送信処理の詳細は、図66のフローチャートを参照して後述する。ステップS45において、ユーザホームネットワーク5の購入モジュール94は、購入処理を実行する。購入処理の詳細は、図67のフローチャートを参照して後述する。ステップS46において、ユーザは、ユーザホームネットワーク5の機器でコンテンツを再生する。再生処理の詳細は、図72のフローチャートを参照して後述する。

#### 【0206】

図57は、図56のS40に対応する、電子配信サービスセンタ1がコンテンツプロバイダ2へ個別鍵 $K_i$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ および公開鍵証明書を送信し、コンテンツプロバイダ2がこれを受信する処理の詳細を説明するフローチャートである。ステップS50において、電子配信サービスセンタ1の相互認証部17は、コンテンツプロバイダ2の相互認証部39と相互認証する。この相互認証処理は、図52で説明したので、その詳細は省略する。相互認証処理により、コンテンツプロバイダ2が正当なプロバイダであることが確認されたとき、ステップS51において、コンテンツプロバイダ2は、電子配信サービスセンタ1のコンテンツプロバイダ管理部12から送信された個別鍵 $K_i$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ および証明書を受信する。ステップS52において、コンテンツプロバイダ2は受信した個別鍵 $K_i$ を耐タンパメモリ40A

に保存し、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  および証明書をメモリ 40B に保存する。

#### 【0207】

このように、コンテンツプロバイダ 2 は、電子配信サービスセンタ 1 から個別鍵  $K_i$  、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  および証明書を受け取る。同様に、図 56 に示すフローチャートの処理を行う例の場合、コンテンツプロバイダ 2 以外に、サービスプロバイダ 3 も、図 57 と同様の処理で、電子配信サービスセンタ 1 から個別鍵  $K_i$  （コンテンツプロバイダ 2 の個別鍵  $K_i$  とは異なる）、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  および証明書を受け取る。

#### 【0208】

なお、メモリ 40A は、コンテンツプロバイダ 2 が秘密裏に保持しなくてはならない個別鍵  $K_i$  を保持するため、第 3 者に容易にデータを読み出されない耐タンパメモリが望ましいが、特にハードウェア的制限は必要ない（例えば、入室管理された部屋の中にあるハードディスクや、パスワード管理されたパソコンのハードディスク等でよい）。また、メモリ 40B は、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  、コンテンツプロバイダ 2 の証明書が保存されるだけであるため、通常の記憶装置等何でもよい（秘密にする必要がない）。また、メモリ 40A、40B を一つにしてもかまわない。

#### 【0209】

図 58 は、ホームサーバ 51 が、電子配信サービスセンタ 1 のユーザ管理部 18 に決済情報を登録する処理を説明するフローチャートである。ステップ S60において、ホームサーバ 51 は、大容量記憶部 68 に記憶されている公開鍵証明書を、暗号処理部 65 の相互認証モジュール 95 で、電子配信サービスセンタ 1 の相互認証部 17 と相互認証する。この認証処理は、図 52 を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップ S60 で、ホームサーバ 51 が電子配信サービスセンタ 1 のユーザ管理部 18 に送信する証明書は、図 32 に示すデータ（ユーザ機器の公開鍵証明書）を含む。

#### 【0210】

ステップ S61において、ホームサーバは個人の決済情報（ユーザのクレジッ

トカード番号や、決済機関の口座番号等)の登録が新規登録か否かを判定し、新規登録であると判定された場合、ステップS62に進む。ステップS62において、ユーザは入力手段63を用いて個人の決済情報を入力する。これらのデータは、暗号化ユニット112で一時鍵K<sub>temp</sub>を用いて暗号化され、通信部61を介して電子配信サービスセンタ1のユーザ管理部18に送信される。

#### 【0211】

ステップS63において、電子配信サービスセンタ1のユーザ管理部18は、受信した証明書から機器のIDを取り出し、この機器のIDを基に、図7に示したユーザ登録データベースを検索する。ステップS64において、電子配信サービスセンタ1のユーザ管理部18は、受信したIDを有する機器の登録が可能であるか否かを判定し、受信したIDを有する機器の登録が可能であると判定された場合、ステップS65に進み、受信したIDを有する機器が、新規登録であるか否かを判定する。ステップS65において、受信したIDを有する機器が、新規登録であると判定された場合には、ステップS66に進む。

#### 【0212】

ステップS66において、電子配信サービスセンタ1のユーザ管理部18は、決済IDを新規に発行すると共に、一時鍵で暗号化された決済情報を復号化し、決済IDおよび決済情報を、機器ID、決済ID、決済情報(口座番号やクレジットカード番号等)、取引停止情報等を記憶している決済情報データベースに機器のIDに対応させて登録し、決済IDをユーザ登録データベースに登録する。ステップ67において、ユーザ登録データベースに登録したデータに基づき登録情報を作成する。この登録情報は、図8で説明しているので、その詳細は省略する。

#### 【0213】

ステップS68において、電子配信サービスセンタ1のユーザ管理部18は、作成した登録情報をホームサーバ51に送信する。ステップS69において、ホームサーバ51の上位コントローラ62は、受信した登録情報を大容量記憶部68に保存する。

## 【0214】

ステップS61において、決済情報の登録が更新登録であると判定された場合、手続きは、ステップS70に進み、ユーザは入力手段63を用いて個人の決済情報を入力する。これらのデータは、暗号化ユニット112で一時鍵K<sub>temp</sub>を用いて暗号化され、既に決済登録時に発行された登録情報と共に通信部61を介して電子配信サービスセンタ1のユーザ管理部18に送信される。

## 【0215】

ステップS64において、受信したIDを有する機器の登録が不可であると判定された場合、ステップS71に進み、電子配信サービスセンタ1のユーザ管理部18は、登録拒絶の登録情報を作成し、ステップS68に進む。

## 【0216】

ステップS65において、受信したIDを有する機器が、新規登録でないと判定された場合、手続きは、ステップS72に進み、電子配信サービスセンタ1のユーザ管理部18は、一時鍵で暗号化された決済情報を復号化し、機器のIDに対応させて決済情報登録データベースに更新登録し、ステップS67に進む。

## 【0217】

このように、ホームサーバ51は、電子配信サービスセンタ1に登録される。

## 【0218】

図59は、登録情報に機器のIDを新規登録する処理を説明するフローチャートである。ステップS80における相互認証処理は、図52で説明した処理と同様なため、説明を省略する。ステップS81において、図58のステップS63と同じであるためその説明は省略する。ステップS82は、図58のステップS64と同じであるためその説明は省略する。ステップS83において、電子配信サービスセンタ1のユーザ管理部18は、ユーザ登録データベース内の機器IDに対応する登録項目を「登録」に設定し、機器IDを登録する。ステップS84において、電子配信サービスセンタ1のユーザ管理部18は、ユーザ登録データベースに基づき、図8に示すような登録情報を作成する。ステップS85は、図58のステップS68と同じであるためその説明は省略する。ステップS86は、図58のステップS69と同じであるためその説明は省略する。

【0219】

ステップS82において、受信したIDを有する機器の登録が不可であると判定された場合、ステップS87に進み、電子配信サービスセンタ1のユーザ管理部18は、登録拒絶の登録情報を作成し、ステップS85に進む。

【0220】

このように、ホームサーバ51は、電子配信サービスセンタ1に登録される。

【0221】

図60は、既に登録された機器を経由し、別の機器を追加登録する際の処理を説明するフローチャートである。ここでは、ホームサーバ51が既に登録されており、そこに据置機器52を登録する例で説明する。ステップS90において、ホームサーバ51は、据置機器52と相互認証する。相互認証処理は、図52で説明した処理と同様なため、説明を省略する。ステップS91において、ホームサーバ51は、電子配信サービスセンタ1と相互認証する。ステップS92において、ホームサーバ51は、大容量記憶部68から読み出した登録情報、およびステップS90で据置機器52と相互認証した際に入手した据置機器52の証明書を電子配信サービスセンタ1に送信する。ステップS93は、図59のステップS81と同じであるためその説明は省略する。ステップS94は、図59のステップS82と同じであるためその説明は省略する。ステップS95は、図59のステップS83と同じであるためその説明は省略する。ステップS96において、電子配信サービスセンタ1のユーザ管理部18は、ホームサーバ51から受信した登録情報に加え、据置機器52の情報を追加した登録情報を新規に作成する。ステップS97は、図59のステップS85と同じであるためその説明は省略する。ステップS98は、図59のステップS86と同じであるためその説明は省略する。

【0222】

そして、ステップS99Aにおいてホームサーバ51は受信した登録情報を据置機器52に送信し、ステップS99Bにおいて据置機器52は受信した登録情報を小容量記憶部75に保存する。

## 【0223】

ステップS94において、受信したIDを有する機器の登録が不可であると判定された場合、ステップS99に進み、電子配信サービスセンタ1のユーザ管理部18は、据置機器52のみ登録拒絶とした登録情報（従って、ホームサーバ51は登録済みのまま）を作成し、ステップS97に進む（ステップS91でホームサーバ51が電子配信サービスセンタ1と相互認証に成功しているということは、ホームサーバ51が登録可であることを意味している）。

## 【0224】

かくして、据置機器52は、図60に示した処理手順により電子配信サービスセンタ1に追加登録される。

## 【0225】

ここで、登録済の機器が登録の更新（登録情報の更新）を行うタイミングについて説明する。図61は登録情報の更新を行うか否かを種々の条件に基づいて判断する処理手順を示し、ステップS600においてホームサーバ51は配送鍵K<sub>d</sub>、登録情報又は課金情報のすい上げから予め決められた一定期間が経過したか否かを時計（図示せず）及び判断部（図示せず）によって判断する。ここで肯定結果が得られると、このことは配送鍵K<sub>d</sub>、登録情報又は課金情報のすい上げから一定の期間が経過していることを表しており、このときホームサーバ51はステップS607に移って登録情報の更新処理を実行する。この処理については図62において後述する。

## 【0226】

これに対してステップS600において否定結果が得られると、このことは配送鍵K<sub>d</sub>、登録情報又は課金情報のすい上げから一定の期間が経過していないこと、すなわち期間の経過について登録情報の更新条件を満たしていないことを表しており、このときホームサーバ51はステップS601に移る。

## 【0227】

ステップS601においてホームサーバ51は、コンテンツの購入回数が規定の回数に達しているか否かを判断する。ここで肯定結果が得られると、ホームサーバ51はステップS607に移って登録情報更新処理を実行し、これに対して

ステップS601において否定結果が得られると、このことはコンテンツの購入回数について登録情報の更新条件を満たしていないことを表していることによりホームサーバ51は続くステップS602に移る。

## 【0228】

ステップS602において、ホームサーバ51は、コンテンツの購入金額が規定の金額に達しているか否かを判断する。ここで肯定結果が得れらると、ホームサーバ51はステップS607に移って登録情報更新処理を実行し、これに対してステップS602において否定結果が得られると、このことはコンテンツの購入金額について登録情報の更新条件を満たしていないことを表していることによりホームサーバ51は続くステップS603に移る。

## 【0229】

ステップS603において、ホームサーバ51は、配送鍵K<sub>d</sub>の有効期限が切れているか否かを判断する。配送鍵K<sub>d</sub>の有効期限が切れているか否かを判断する方法としては、配信されたデータの配送鍵K<sub>d</sub>のバージョンが記憶モジュール92に保存されている3つのバージョンの配送鍵K<sub>d</sub>のいずれかのバージョンと一致するか否か又は、最近の配送鍵K<sub>d</sub>のバージョンより古いか否かを調べる。この比較結果が一致していない場合又は最近の配送鍵K<sub>d</sub>のバージョンより古い場合には、記憶モジュール92内の配送鍵K<sub>d</sub>の有効期限が切れていることになり、ホームサーバ51はステップS603において肯定結果を得ることによりステップS607に移って登録情報の更新処理を実行する。これに対してステップS603において否定結果が得られると、このことは配送鍵K<sub>d</sub>の有効期限について登録情報の更新条件を満たしていないことを表しており、このときホームサーバ51は続くステップS604に移る。

## 【0230】

ステップS604において、ホームサーバ51は、当該ホームサーバ51に他機器が新規接続されたか否か、又は接続されていた他機器が切り離されたか否かといったネットワーク構成の変更の有無を判断する。ここで肯定結果が得られると、このことはネットワーク構成に変更があったことを表しており、このときホームサーバ51はステップS607に移って登録情報の更新処理を実行する。こ

れに対してステップS604において否定結果が得られると、このことはネットワーク構成について登録情報の更新条件を満たしていないことを表しており、ホームサーバ51は続くステップS605に移る。

#### 【0231】

ステップS605において、ホームサーバ51は、ユーザからの登録情報更新要求があったか否かを判断し、登録情報更新要求があった場合にはステップS607に移って登録情報の更新処理を実行し、登録情報更新要求がなかった場合にはステップS606に移る。

#### 【0232】

ステップS606において、ホームサーバ51は接続された他の機器について上述のステップS600～ステップS605における更新判断を行い、更新すべき判断結果が得られたときステップS607に移って登録情報の更新処理を行い、これに対して更新すべき判断結果が得られないとき上述のステップS600から同様の処理を繰り返す。これにより、ホームサーバ51は登録情報の更新処理を行うタイミングを得ることができる。なお、ホームサーバ51が他の機器の更新開始条件を調べるのではなく、他の機器が独自に調べて、自らホームサーバ51に要求を出すようにしてもよい。

#### 【0233】

図62は、登録済みの機器が登録を更新（登録情報の更新）し、決済処を行、配送鍵 $K_d$ の再配布を受ける動作を説明するフローチャートである。ステップS100における相互認証処理は、図52で説明した処理と同様なため、説明を省略する。ステップS101において、ホームサーバ51は、記憶モジュール92に記憶されている課金情報を、暗号処理部96の暗号化ユニット112で一時鍵 $K_{temp}$ を用いて暗号化し、署名生成ユニット114で署名を生成し、署名を付加する。そして、暗号化された課金情報及びその署名と、大容量記憶部68に記憶されている取扱方針、価格情報および登録情報を合わせて電子配信サービスセンタ1に送信する。なお、このとき、取扱方針および価格情報はモデルによっては送信する必要がない。なぜなら、コンテンツプロバイダ2およびサービスプロバイダ3が予め電子配信サービスセンタ1に送信している場合があったり、課

金情報に取扱方針、価格情報のうちの必要な情報が含まれている場合があるからである。

#### 【0234】

ステップS102は、図59のステップS81と同じであるためその説明は省略する。ステップS103は、図59のステップS82と同じであるためその説明は省略する。ステップS104において、電子配信サービスセンタ1のユーザ管理部18は署名検証ユニット115で署名を検証し、受信した課金情報を一時鍵K<sub>temp</sub>で復号化し（受信データに電子署名がついている場合には、署名検証ユニット115で検証する）、（受信していれば）取扱方針および価格情報と共に経歴データ管理部15に送信する。これを受信した経歴データ管理部15は、受信データを保存・管理する。

#### 【0235】

ステップS105において、電子配信サービスセンタ1のユーザ管理部18は、ユーザ登録データベース内の機器IDに対応する登録項目を検証すると共に、データを更新する。例えば、図示せぬ登録日付や課金状況などのデータである。ステップS106は、図59のステップS84と同じであるためその説明は省略する。ステップS107において、電子配信サービスセンタ1のユーザ管理部は、鍵サーバ14から供給された配送鍵K<sub>d</sub>を一時鍵K<sub>temp</sub>で暗号化し、登録情報と共にホームサーバ51に送信する。

#### 【0236】

ステップS108において、ホームサーバ51は受信した登録情報を大容量記憶部68に保存する。ステップS109において、ホームサーバ51は、受信した登録情報を暗号処理部65に入力し、暗号処理部65では、登録情報に含まれる電子署名を署名検証ユニット115で検証すると共に、ホームサーバ51の機器IDが登録されているか確認させ、検証に成功し、課金処理が完了したことを見認めた際にはステップS110に進む。ステップS110において、ホームサーバ51は、受信した配送鍵K<sub>d</sub>を暗号処理部65に入力する。暗号処理部65では、受信した配送鍵K<sub>d</sub>を暗号／復号化モジュール96の復号化ユニット111で一時鍵K<sub>temp</sub>を用いて復号化し、記憶モジュール92に保存（更新）し、記

憶モジュール92に保持していた課金情報を消去する（これで、決済済みとなる）。

#### 【0237】

ステップS103において、受信したIDを有する機器の登録が不可であると判定された場合、ステップS111に進み、電子配信サービスセンタ1のユーザ管理部18は、登録拒絶とした登録情報を作成し、ステップS112に進む。ステップS112では、ステップS107と異なり、登録情報のみをホームサーバ51に送信する。

#### 【0238】

ステップS109において、登録情報に含まれる署名の検証に失敗するか、登録情報に含まれる「登録」の項目（例えば、課金処理失敗→購入処理ができない、登録拒否→再生等の処理を含め暗号処理部の機能の停止、取引一時停止→課金処理は成功したが、何らかの理由で購入を停止する、等が考えられる）に「登録可」が書かれていない場合は、ステップS113に進み所定のエラー処理を行う。

#### 【0239】

このように、ホームサーバ51は、登録情報を更新すると共に、課金情報を電子配信サービスセンタ1に送信し、代わりに配送鍵K<sub>d</sub>の供給を受ける。

#### 【0240】

図63及び図64は、据置機器52がホームサーバ51を介して決済、登録情報の更新、配送鍵K<sub>d</sub>の更新を行う処理を説明するフローチャートを示した図である。ステップS120において、ホームサーバ51の相互認証モジュール94と据置機器の図示せぬ相互認証モジュールは、相互認証を行う。相互認証処理は、図52で説明した処理と同様なため、説明を省略する。なお、相互認証処理で説明したように、ホームサーバ51と据置機器52は互いに証明書を交換し合っているため、相手の機器IDはわかっているものとする。ステップS121において、ホームサーバ51の上位コントローラ62は、大容量記憶部68から登録情報を読み出し、暗号処理部65に検査させる。上位コントローラ62から登録情報を受け取った暗号処理部65は、登録情報内の署名を検証し、据置機器のI

Dがあるかどうか判定し、登録情報に据置機器のIDがあった際にはステップS122に進む。

#### 【0241】

ステップS122において、登録情報に据置機器52のIDが登録されているか否かを判定し、据置機器52のIDが登録されている場合には、ステップS123に進む。ステップS123において、据置機器52の暗号処理部73は、記憶モジュールに保存されている課金情報を読み出し、暗号化ユニットで一時鍵K<sub>temp</sub>を用いて暗号化する。また、課金情報に対応する署名を、署名生成ユニットで生成する。署名の生成は図10で説明したのでその詳細は省略する。一時鍵K<sub>temp</sub>で暗号化された課金情報およびその署名を受け取った上位コントローラ72は、必要に応じて課金情報に対応する取扱方針および価格情報を小容量記憶部75から読み出し、一時鍵K<sub>temp</sub>で暗号化された課金情報とその署名、必要に応じて課金情報に対応する取扱方針および価格情報をホームサーバ51に送信する。

#### 【0242】

これらのデータを受信したホームサーバ51は、受信していれば取扱方針および価格情報を大容量記憶部68に記憶すると共に、一時鍵K<sub>temp</sub>で暗号化された課金情報およびその署名を暗号処理部65に入力する。一時鍵K<sub>temp</sub>で暗号化された課金情報およびその署名を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で、一時鍵K<sub>temp</sub>で暗号化された課金情報に対する署名を検証する。署名の検証は図11で説明したの処理と同じであるため、その詳細は省略する。そして、暗号／復号化モジュール96の復号化ユニット111は、一時鍵K<sub>temp</sub>で暗号化された課金情報を復号化する。

#### 【0243】

ステップS124において、ホームサーバ51は、電子配信サービスセンタ1の相互認証部17と相互認証し一時鍵K<sub>temp</sub>2を共有する。ステップS125において、ホームサーバ51は、据置機器52から送られたきた課金情報を暗号／復号化モジュール96の暗号化ユニット112で一時鍵K<sub>temp</sub>2を用いて暗号化する。このとき、ホームサーバ51の課金情報を合わせて暗号化しておいてよい。また、一時鍵K<sub>temp</sub>2で暗号化された課金情報に対応する署名を、暗号／復

号化モジュール96の署名生成ユニット114で生成する。一時鍵K<sub>temp</sub>2で暗号化された課金情報、およびその署名を受け取った上位コントローラ62は、必要に応じて課金情報に対応する取扱方針、価格情報、および登録情報を大容量記憶部68から読み出し、一時鍵K<sub>temp</sub>2で暗号化された課金情報、その署名、必要に応じて課金情報に対応する取扱方針、価格情報および登録情報を電子配信サービスセンタ1のユーザ管理部18に送信する。

#### 【0244】

ステップS126において、電子配信サービスセンタ1のユーザ管理部18は、ユーザ登録データベースを検索する。ステップS127において、ホームサーバ51および据置機器52がユーザ登録データベース内の「登録」の項目に、登録可で登録されているか否か判定し、登録されていると判定されていた場合、ステップS128に進む。ステップS128において、電子配信サービスセンタ1のユーザ管理部18は、一時鍵K<sub>temp</sub>2で暗号化された課金情報に対する署名を検証し、課金情報を一時鍵K<sub>temp</sub>2で復号化する。そして、課金情報、受信していれば取扱方針および価格情報を経歴データ管理部15に送信する。課金情報、受信していれば取扱方針および価格情報を受信した経歴データ管理部15は、そのデータを管理・保存する。

#### 【0245】

ステップS129において、電子配信サービスセンタ1のユーザ管理部18は、ユーザ登録データベースを更新する（図示せぬ課金データ受信日時、登録情報発行日時、配送鍵交付日時等）。ステップS130において、電子配信サービスセンタ1のユーザ管理部18は、登録情報を作成する（例えば図8の例）。ステップS131において、電子配信サービスセンタ1の鍵サーバ14から受信した配送鍵K<sub>d</sub>を一時鍵K<sub>temp</sub>2で暗号化し、一時鍵K<sub>temp</sub>2で暗号化された配送鍵K<sub>d</sub>に対する署名を生成する。そして、登録情報、一時鍵K<sub>temp</sub>2で暗号化された配送鍵K<sub>d</sub>および一時鍵K<sub>temp</sub>2で暗号化された配送鍵K<sub>d</sub>に対する署名をホームサーバ51に送信する。

#### 【0246】

ステップS132において、ホームサーバ51は、登録情報、一時鍵K<sub>temp</sub>2

で暗号化された配送鍵  $K_d$  および一時鍵  $K_{temp}^2$  で暗号化された配送鍵  $K_d$  に対する署名を受信する。ホームサーバ 51 の上位コントローラ 62 は、一時鍵  $K_{temp}^2$  で暗号化された配送鍵  $K_d$  および一時鍵  $K_{temp}^2$  で暗号化された配送鍵  $K_d$  に対する署名を暗号処理部 65 に入力する。暗号処理部 65 において、暗号／復号化モジュール 96 の署名検証ユニット 115 は、一時鍵  $K_{temp}^2$  で暗号化された配送鍵  $K_d$  に対する署名を検証し、暗号／復号化モジュール 96 の復号化ユニット 111 は、一時鍵  $K_{temp}^2$  を用いて配送鍵  $K_d$  を復号化し、暗号／復号化モジュール 96 の暗号化ユニット 112 は、復号化された配送鍵  $K_d$  を、据置機器 52 との間で共有した一時鍵  $K_{temp}$  を用いて再暗号化する。最後に、暗号／復号化モジュール 96 の署名生成ユニット 114 は、一時鍵  $K_{temp}$  を用いて暗号化された配送鍵  $K_d$  に対する署名を生成し、一時鍵  $K_{temp}$  で暗号化された配送鍵  $K_d$  および一時鍵  $K_{temp}$  で暗号化された配送鍵  $K_d$  に対する署名を上位コントローラ 62 に返送する。一時鍵  $K_{temp}$  で暗号化された配送鍵  $K_d$  および一時鍵  $K_{temp}$  で暗号化された配送鍵  $K_d$  に対する署名を受信した上位コントローラ 62 は、電子配信サービスセンタ 1 から送られた来た登録情報と共に据置機器 52 に送信する。

#### 【0247】

ステップ S133において、据置機器 52 の上位コントローラ 72 は、受信した登録情報を小容量記憶部 75 に上書き保存する。ステップ S134において、据置機器 52 の暗号処理部 73 は、受信した登録情報の署名を検証し、据置機器 52 の I.D の「登録」に対する項目が「登録可」になっているか否かを判定し、「登録可」になっていた場合には、ステップ S135 に進む。ステップ S135 において、据置機器 52 の上位コントローラは、一時鍵  $K_{temp}$  で暗号化された配送鍵  $K_d$  および一時鍵  $K_{temp}$  で暗号化された配送鍵  $K_d$  に対する署名を暗号処理部 73 に入力する。暗号処理部 73 は、一時鍵  $K_{temp}$  で暗号化された配送鍵  $K_d$  に対する署名を検証し、一時鍵  $K_{temp}$  を用いて配送鍵  $K_d$  を復号化し、暗号処理部 73 の記憶モジュール内の配送鍵  $K_d$  を更新すると共に、課金情報を消去する（なお、実際には消去せず、決済済みのマークを付けるだけの場合がある）。

## 【0248】

ステップS121において、据置機器52のIDが登録情報に含まれていなかった場合、ステップS136に進み、図60で説明した登録情報追加処理を開始し、ステップS123へと進む。

## 【0249】

ステップS127において、ユーザ登録データベース内の「登録」項目に対し、ホームサーバ51のIDまたは据置機器52のIDが「登録可」になっていた場合、ステップS137に進む。ステップS137は、ステップS130の場合と同様なため、その詳細は省略する。ステップS138は、ステップS131において、電子配信サービスセンタ1のユーザ管理部18は、登録情報をホームサーバ51に送信する。ステップS139において、ホームサーバ51は、登録情報を据置機器52に送信する。

## 【0250】

ステップS122において、登録情報における据置機器52のIDに対する「登録」項目が、「登録可」になっていた場合、ステップS134において、登録情報における据置機器52のIDに対する「登録」項目が、「登録可」になっていた場合、処理は終了する。

## 【0251】

なお、本方式による代理処理は、据置機器52のみの処理になっているが、ホームサーバ51につながる全ての機器やホームサーバ51自身の課金情報を全て集め、一括処理しても良い。そして、全ての機器の登録情報、配送鍵K<sub>d</sub>の更新を行う（本実施例において、受け取った登録情報、配送鍵K<sub>d</sub>は、ホームサーバ51で全くチェックされていない。ホームサーバ51自身の処理も一括して行う場合には、当然チェックし、更新すべきである）。

## 【0252】

次に、図56のステップS43に対応する、コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュアコンテナを送信する処理を、図65のフローチャートを用いて説明する。ステップS140において、コンテンツプロバイダ2の電子透かし付加部32は、コンテンツサーバ31から読み出し

たコンテンツに、コンテンツプロバイダ2を示す所定のデータ、例えばコンテンツプロバイダIDなどを電子透かしの形で挿入し、圧縮部33に供給する。ステップS141において、コンテンツプロバイダ2の圧縮部33は、電子透かしが挿入されたコンテンツをATRAC等の所定の方式で圧縮し、コンテンツ暗号部34に供給する。ステップS142において、コンテンツ鍵生成部35は、コンテンツ鍵 $K_{co}$ として用いる鍵を生成させ、コンテンツ暗号部34およびコンテンツ鍵暗号部36に供給する。ステップS143において、コンテンツプロバイダ2のコンテンツ暗号部34は、DESなどの所定の方式で、コンテンツ鍵 $K_{co}$ を使用して、電子透かしが挿入され、圧縮されたコンテンツを暗号化する。

#### 【0253】

ステップS144において、コンテンツ鍵暗号部36は、DESなどの所定の方法で、図56のステップS40の処理により、電子配信サービスセンタ1から供給されている個別鍵 $K_i$ でコンテンツ鍵 $K_{co}$ を暗号化する。ステップS145において、取扱方針生成部37は、コンテンツの取り扱い方針を規定し、図33又は図34に示すような取扱方針を生成する。ステップS146において、コンテンツプロバイダ2の署名生成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 $K_{co}$ 、暗号化された個別鍵 $K_i$ および取扱方針生成部37から供給された取扱方針に対し署名を生成する。署名の生成は図10を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS147において、コンテンツプロバイダ2は、暗号化されたコンテンツおよびその署名、暗号化されたコンテンツ鍵 $K_{co}$ およびその署名、暗号化された個別鍵 $K_i$ およびその署名、取扱方針およびその署名（以降、これら4つの署名付きデータをコンテンツプロバイダセキュアコンテナと呼ぶ）、予め認証局からもらつておいたコンテンツプロバイダ2の証明書を、図示せぬ送信部を用いてサービスプロバイダ3に送信する。

#### 【0254】

以上のように、コンテンツプロバイダ2は、サービスプロバイダ3に、コンテンツプロバイダセキュアコンテナを送信する。

## 【0255】

次に、図56のステップS44に対応する、サービスプロバイダ3がホームサーバ51にサービスプロバイダセキュアコンテナを送信する処理を、図66のフローチャートを用いて説明する。なお、サービスプロバイダ3は、コンテンツプロバイダ2から送信されたデータをコンテンツサーバ41に予め保存しているものとして説明する。ステップS150において、サービスプロバイダ3の証明書検証部42は、コンテンツサーバ41からコンテンツプロバイダ2の証明書の署名を読み出し、証明書内の署名を検証する。署名の検証は図11を参照して説明した方法と同様なため、その詳細は省略する。証明書に改竄がなければ、コンテンツプロバイダ2の公開鍵 $K_{pcp}$ を取り出す。

## 【0256】

ステップS151において、サービスプロバイダ3の署名検証部43は、コンテンツプロバイダ2の送信部から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ2の公開鍵 $K_{pcp}$ で検証する（取扱方針の署名のみ検証する場合がある）。署名の検証に失敗し、改竄が発見された場合は、処理を終了する。なお、署名の検証は図11を参照して説明した方法と同様なため、その詳細は省略する。

## 【0257】

コンテンツプロバイダセキュアコンテナに改竄がない場合、ステップS152において、サービスプロバイダ3の値付け部44は、取扱方針を基に、図37や図38で説明した価格情報を作成する。ステップS153において、サービスプロバイダ3の署名生成部45は、価格情報に対する署名を生成し、コンテンツプロバイダセキュアコンテナ、価格情報、および価格情報の署名を合わせサービスプロバイダセキュアコンテナを作成する。

## 【0258】

ステップS154において、サービスプロバイダ3の図示せぬ送信部は、ホームサーバ51の通信部61に、サービスプロバイダ3の証明書、コンテンツプロバイダ2の証明書およびサービスプロバイダセキュアコンテナを送信し、処理を終了する。

## 【0259】

このように、サービスプロバイダ3は、ホームサーバ51にサービスプロバイダセキュアコンテナを送信する。

## 【0260】

図56のステップS45に対応する、適正なサービスプロバイダセキュアコンテナを受信した後の、ホームサーバ51の購入処理の詳細を、図67のフローチャートを用いて説明する。ステップS161において、ホームサーバ51は図61及び図62について上述した登録情報更新処理を実行した後、ステップS162において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した登録情報をホームサーバ51の暗号処理部65に入力する。登録情報を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で登録情報の署名を検証した後、ホームサーバ51のIDに対する「購入処理」の項目が「購入可」になっているか判定すると共に登録の項目を「登録可」になっていることを検査し、「購入可」及び「登録可」であった場合にはステップS163に進む。なお、署名検証、「登録可」、「購入可」の検査は登録情報検査モジュール93で行うようにしても良い。ステップS163において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツプロバイダ2の公開鍵証明書をホームサーバ51の暗号処理部65に入力する。

## 【0261】

コンテンツプロバイダ2の公開鍵証明書を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツプロバイダ2の証明書の署名を検証した後、公開鍵証明書からコンテンツプロバイダ2の公開鍵を取り出す。署名の検証の結果、改竄がなされていないことが確認された場合には、ステップS164に進む。ステップS164において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツをホームサーバ51の暗号処理部65に入力する。コンテンツを受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツの署名を検証し、改竄がなされていないことが確認された場合には、

ステップS165に進む。ステップS165において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツ鍵K<sub>co</sub>をホームサーバ51の暗号処理部65に入力する。

#### 【0262】

コンテンツ鍵K<sub>co</sub>を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツ鍵K<sub>co</sub>の署名を検証し、改竄がなされていないことが確認された場合には、ステップS166に進む。ステップS166において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した個別鍵K<sub>i</sub>をホームサーバ51の暗号処理部65に入力する。個別鍵K<sub>i</sub>を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で個別鍵K<sub>i</sub>の署名を検証し、改竄がなされていないことが確認された場合には、ステップS167に進む。

#### 【0263】

ステップS167において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した取扱方針をホームサーバ51の暗号処理部65に入力する。取扱方針を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で取扱方針の署名を検証し、改竄がなされていないことが確認された場合には、ステップS168に進む。ステップS168において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したサービスプロバイダ3の公開鍵証明書をホームサーバ51の暗号処理部65に入力する。

#### 【0264】

サービスプロバイダ3の公開鍵証明書を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でサービスプロバイダ3の証明書の署名を検証した後、公開鍵証明書からサービスプロバイダ3の公開鍵を取り出す。署名の検証の結果、改竄がなされていないことが確認された場合には、ステップS169に進む。ステップS169において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した価格情報をホームサーバ51の暗号処理部65に入力する。価格情報を受信した暗号処理

部65は、暗号／復号化モジュール96の署名検証ユニット115で価格情報の署名を検証し、改竄がなされていないことが確認された場合には、ステップS170に進む。

#### 【0265】

ステップS170において、ホームサーバ51の上位コントローラ62は、表示手段64を用いて購入可能なコンテンツの情報（例えば、購入可能な利用形態や価格など）を表示し、ユーザは入力手段63を用いて購入項目を選択する。入力手段63から入力された信号はホームサーバ51の上位コントローラ62に送信され、上位コントローラ62は、その信号に基づいて購入コマンドを生成し、購入コマンドをホームサーバ51の暗号処理部65に入力する。なお、これらの入力処理は購入処理スタート時に行っても良い。これを受信した暗号処理部65は、ステップS167で入力された取扱方針およびステップS169で入力された価格情報から課金情報および使用許諾条件情報を生成する。課金情報については、図42で説明したので、その詳細は省略する。使用許諾条件情報については、図41で説明したので、その詳細は省略する。

#### 【0266】

ステップS171において、暗号処理部65の制御部91は、ステップS170で生成した課金情報を記憶モジュール92に保存する。ステップS172において、暗号処理部65の制御部91は、ステップS170で生成した使用許諾条件情報を暗号処理部65の外部メモリ制御部97に送信する。使用許諾条件情報を受信した外部メモリ制御部97は、外部メモリ67の改竄チェックを行った後、使用許諾条件情報を外部メモリ67に書き込む。書き込む際の改竄チェックについては、図69を用いて後述する。ステップS173において、暗号処理部65の制御部91は、ステップS166で入力された個別鍵 $K_i$ を、暗号／復号化モジュール96の復号化ユニット111で、記憶モジュール92から供給された配達鍵 $K_d$ を用いて復号化する。次に、暗号処理部65の制御部91は、ステップS165で入力されたコンテンツ鍵 $K_{co}$ を、暗号／復号化モジュール96の復号化ユニット111で、先ほど復号化した個別鍵 $K_i$ を用いて復号化する。最後に、暗号処理部65の制御部91は、暗号／復号化モジュール96の暗号化ユニ

ット112で、記憶モジュール92から供給された保存鍵K<sub>save</sub>を用いてコンテンツ鍵K<sub>co</sub>を暗号化する。ステップS174において、保存鍵K<sub>save</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>は、暗号処理部65の外部メモリ制御部97を経由して外部メモリ67に保存される。

#### 【0267】

ステップS162でホームサーバ51が購入処理できない機器であると判定された場合、又はステップS163でコンテンツプロバイダ2の公開鍵証明書の署名が正しくないと判定された場合、又はステップS164でコンテンツ鍵K<sub>co</sub>で暗号化されたコンテンツの署名が正しくないと判定された場合、又はステップS165で個別鍵K<sub>i</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>の署名が正しくないと判定された場合、又はステップS166で配送鍵K<sub>d</sub>で暗号化された個別鍵K<sub>i</sub>の署名が正しくないと判定された場合、又はステップS167で取扱方針の署名が正しくないと判定された場合、又はステップS168でサービスプロバイダ3の証明書の署名が正しくないと判定された場合、又はステップS169で価格情報の署名が正しくないと判定された場合、ホームサーバ51はステップS176に進み、エラー処理を行う。なおステップS165、およびステップS166の処理をまとめ、コンテンツ鍵K<sub>co</sub>、個別鍵K<sub>i</sub>に対する唯一の署名を検証するとしてもよい。

#### 【0268】

以上のように、ホームサーバ51は、課金情報を記憶モジュール92に記憶すると共に、コンテンツ鍵K<sub>co</sub>を個別鍵K<sub>i</sub>で復号化した後、コンテンツ鍵K<sub>co</sub>を保存鍵K<sub>save</sub>で暗号化し、外部メモリ67に記憶させる。

#### 【026.9】

据置機器52も、同様の処理で、課金情報を暗号処理部73の記憶モジュールに記憶すると共に、コンテンツ鍵K<sub>co</sub>を個別鍵K<sub>i</sub>で復号化し、コンテンツ鍵K<sub>co</sub>を保存鍵K<sub>save</sub>2（ホームサーバ51の鍵と異なる）で暗号化し、外部メモリ79に記憶させる。

#### 【0270】

図68は、暗号処理部65の外部メモリ制御部97が、外部メモリ67からデ

ータを読み出す際に行う、改竄チェックの方法を説明するフローチャートである。図68のステップS180において、暗号処理部65の外部メモリ制御部97は、外部メモリ67から読み出すデータの場所を検索する（例えば図16のブロック目の1番目のデータ）。ステップS181において、暗号処理部65の外部メモリ制御部97は、外部メモリ67内の読み出し予定データを含む同一ブロック内全てのデータに対するハッシュ値（図16の1ブロック目全体のハッシュ値）を計算する。このとき、読み出し予定のデータ（例えばコンテンツ鍵1と使用許諾条件情報1）以外は、ハッシュ値計算に使用後、破棄される。ステップS182において、ステップS181で計算したハッシュ値と暗号処理部65の記憶モジュール92に記憶されているハッシュ値（ICV<sub>1</sub>）を比較する。一致していた場合、ステップS181で読み出しておいたデータを、外部メモリ制御部97を介して制御部91に送信し、一致ていなかつた場合、外部メモリ制御部97はS183に移り、当該メモリブロックは改竄されているものとして以降の読み書きを禁止する（不良ブロックとする）。例えば、外部メモリを4MBのフラッシュメモリとしたとき、このメモリを64のブロックに分けたものと仮定する。従って、記憶モジュールには64個のハッシュ値が記憶されている。データの読み出しを行う場合は、まず、データがある場所を検索し、そのデータを含む同一ブロック内全てのデータに対するハッシュ値を計算する。このハッシュ値が、記憶モジュール内の当該ロックに対応したハッシュ値と一致しているか否かで改竄をチェックする（図16参照）。

#### 【0271】

このように、暗号処理部65の外部メモリ制御部97は、外部メモリ67の改竄チェックを行い、データを読み出す。

#### 【0272】

図69は、暗号処理部65の外部メモリ制御部97が、外部メモリ67にデータを書き込む際に行う、改竄チェックの方法を説明するフローチャートである。図69のステップS190Aにおいて、暗号処理部65の外部メモリ制御部97は、外部メモリ67にデータを書き込むことができる場所を検索する。ステップS191Aにおいて、暗号処理部65の外部メモリ制御部97は、外部メモリ6

7 内に空きエリアがあるか否か判定し、空きエリアがあると判定した場合、ステップS192Aに進む。ステップS192Aにおいて、暗号処理部65の外部メモリ制御部97は、書き込み予定データブロック内の、全てのデータに対するハッシュ値を計算する。ステップS193Aにおいて、ステップS192Aで計算したハッシュ値と暗号処理部65の記憶モジュール92に記憶されているハッシュ値を比較し、一致していた場合、ステップS194Aに進む。ステップS194Aにおいて、書き込み予定領域にデータを書き込む。ステップS195Aにおいて、暗号処理部65の外部メモリ制御部97は、書き込んだデータブロック内の、全てのデータに対するハッシュ値を再計算する。ステップS196Aにおいて、制御部91は、暗号処理部65の記憶モジュール92内のハッシュ値をステップS195Aで計算したハッシュ値に更新する。

#### 【0273】

ステップS193Aにおいて、計算したハッシュ値が記憶モジュール92内のハッシュ値と異なっていた場合、制御部91は、そのメモリブロックを不良ブロックとし（例えば、ハッシュ値を不良ブロックを示す値に変更する）、ステップS190Aへ進む。

#### 【0274】

ステップS191Aにおいて、外部メモリ67に空きエリアがないと判定された場合、ステップS198Aに進み、ステップS198Aにおいて、外部メモリ制御部97は、書き込みエラーを制御部91に返送し、処理を終了する。

#### 【0275】

外部メモリ制御部97の外部メモリ67への書き換え（更新）方法は、図70に示すように、ステップS190Bにおいて暗号処理部65の外部メモリ制御部97は、外部メモリ67のデータを書き換える場所を検索する。ステップS192Bにおいて、暗号処理部65の外部メモリ制御部97は、書き換え予定データブロック内の、全てのデータに対するハッシュ値を計算する。ステップS193Bにおいて、ステップS192Bで計算したハッシュ値と暗号処理部65の記憶モジュール92に記憶されているハッシュ値を比較し、一致していた場合、ステップS194Bに進む。ステップS194Bにおいて、書き換え予定領域のデータ

タを書き換える。ステップS195Bにおいて、暗号処理部65の外部メモリ制御部97は、書き込んだデータブロック内の、全てのデータに対するハッシュ値を再計算する。ステップS196Bにおいて、制御部91は、暗号処理部65の記憶モジュール92内のハッシュ値をステップS195Bで計算したハッシュ値に更新する。

#### 【0276】

ステップS193Bにおいて、計算したハッシュ値が記憶モジュール92内のハッシュ値と異なっていた場合、制御部91は、そのメモリブロックを不良ブロックとし（例えば、ハッシュ値とを不良ブロックを示す値に変更する）、書き換え失敗とする。

#### 【0277】

外部メモリ79のデータの削除方法について、図71を用いて説明する。ステップS190Cにおいて、暗号処理部73の外部メモリ制御部は、外部メモリ79のデータを削除する場所を検索する。ステップS192Cにおいて、暗号処理部73の外部メモリ制御部は、データ削除予定データブロック内の、全てのデータに対するハッシュ値とを計算する。ステップS193Cにおいて、ステップS192Cで計算したハッシュ値と暗号処理部73の記憶モジュール（図示せず）に記憶されているハッシュ値を比較し、一致していた場合、ステップS194Cに進む。ステップS194Cにおいて、削除予定領域の削除予定であるデータを削除する。ステップS195Cにおいて、暗号処理部73の外部メモリ制御部は、削除予定データを削除したデータブロック内の、全てのデータに対するハッシュ値を再計算する。ステップS196Cにおいて、暗号処理部73は記憶モジュール内のハッシュ値をステップS195Cで計算したハッシュ値に更新する。

#### 【0278】

ステップS193Cにおいて、計算したハッシュ値が記憶モジュール内のハッシュ値と異なっていた場合、暗号処理部73は、そのメモリブロックを不良ブロックとし（例えば、ハッシュ値とを不良ブロックを示す値に変更する）、消去失敗とする。

## 【0279】

図56のステップS46に対応するホームサーバ51がコンテンツを再生する処理の詳細を、図72及び図73のフローチャートを用いて説明する。ステップS200において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の入力手段63から再生指示されたコンテンツに対応するIDを、ホームサーバ51の暗号処理部65に入力する。ステップS201において、再生するコンテンツIDを受信した暗号処理部65の制御部91は、コンテンツIDを暗号処理部65の外部メモリ制御部97に送信し、コンテンツIDに対応するコンテンツ鍵K<sub>c0</sub>および使用許諾条件情報を検索させる。このとき、使用許諾条件情報が再生可能な権利であることを確認する。ステップS202において、暗号処理部65の外部メモリ制御部97は、コンテンツ鍵K<sub>c0</sub>および使用許諾条件情報を含むデータブロックのハッシュ値を計算し、暗号処理部65の制御部91に送信する。ステップS203において、暗号処理部65の制御部91は、暗号処理部65の記憶モジュール92に記憶されているハッシュ値とステップS202で受信したハッシュ値が一致しているか否か判定し、一致していた場合にはステップS204に進む。

## 【0280】

ステップS204において、暗号処理部65の制御部91は、使用許諾条件情報を必要に応じて更新する。例えば、使用許諾条件情報内の利用権が回数券であった場合、その回数を減算するなどの処理である。従って、更新する必要のない買い切りの権利などは、更新する必要がなく、その場合、ステップS208へジャンプする（図示していない）。ステップS205において、外部メモリ制御部97は、制御部91から送信された更新された使用許諾条件情報を、外部メモリ67に書き換え更新する。ステップS206において、外部制御部97は、書き換えたデータブロック内の全データに対するハッシュ値を計算し直し、暗号処理部65の制御部91に送信する。ステップS207において、暗号処理部65の制御部91は、暗号処理部65の記憶モジュール92に記憶されているハッシュ値を、ステップS206で算出したハッシュ値に書き換える。

## 【0281】

ステップS208において、暗号処理部65と伸張部66は相互認証を行い、一時鍵K<sub>temp</sub>を共有する。相互認証処理は、図51を用いて説明したのでその詳細は省略する。ステップS209において、暗号／復号化モジュール96の復号化ユニット111は、外部メモリ97から読み出したコンテンツ鍵K<sub>c0</sub>を、記憶モジュール92から供給された保存鍵K<sub>save</sub>で復号化する。ステップS210において、暗号／復号化モジュール96の暗号化ユニット112は、先ほど伸張部66と共有した一時鍵K<sub>temp</sub>でコンテンツ鍵K<sub>c0</sub>を再暗号化する。ステップS211において、暗号処理部65の制御部91は、上位コントローラ62を介して、一時鍵K<sub>temp</sub>で暗号化されたコンテンツ鍵K<sub>c0</sub>を伸張部66に送信する。

## 【0282】

ステップS212において、伸張部66の鍵復号モジュール102は、相互認証モジュール101から供給された一時鍵K<sub>temp</sub>でコンテンツ鍵K<sub>c0</sub>を復号化する。ステップS213において、上位コントローラ62は大容量記憶部68からコンテンツを読み出し、伸張部66に供給する。コンテンツを受信した伸張部66の復号モジュール103は、鍵復号モジュール102から供給されたコンテンツ鍵K<sub>c0</sub>を用いてコンテンツを復号化する。ステップS214において、伸張部66の伸張モジュール104は、コンテンツを所定の方式、例えばATRACなどの方式により伸張する。ステップS215において、電子透かし付加モジュール105は、暗号処理部65から指示されたデータを電子透かしの形でコンテンツに挿入する（暗号処理部から伸張部へ渡されるデータは、コンテンツ鍵K<sub>c0</sub>だけではなく、再生条件（アナログ出力、デジタル出力、コピー制御信号付き出力(SCMS)）、コンテンツ利用権を購入した機器IDなども含まれている。挿入するデータは、このコンテンツ利用権を購入した機器のID（つまりは、使用許諾条件情報内の機器ID）などである）。ステップS216において、伸張部66は、図示せぬスピーカを介して音楽を再生する。

## 【0283】

このように、ホームサーバ51は、コンテンツを再生する。

## 【0284】

図74は、ホームサーバ51が据置機器52のために、コンテンツ利用権を代理購入する処理の詳細を説明したフローチャートである。ステップS220において、ホームサーバ51と据置機器52は、相互認証する。相互認証処理は、図52で説明した処理と同様なため、説明を省略する。ステップS221において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した登録情報を、ホームサーバ51の暗号処理部65に検査させる。上位コントローラ62から登録情報を受信した暗号処理部65は、暗号/復号化モジュール96の署名検証ユニット115に、登録情報に付加されている署名を、暗号処理部65の記憶モジュール92から供給された電子配信サービスセンタ1の公開鍵で検証させる。署名の検証に成功した後、暗号処理部65の制御部91は、登録情報に据置機器のIDが登録され、「登録」及び「購入」の項目が「登録可」と「購入化」になっているか判定し、「登録可」になっていると判定された場合にはステップS222に進む（なお、据置機器52側でも登録情報を検査し、ホームサーバ51が「登録可」になっていることを判定している）。ステップS225からステップS227は、図67のステップS160からステップS171までと同様な処理なため、その詳細は省略する。

## 【0285】

ステップS228において、暗号処理部65の制御部91は、ステップS225で入力された配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を、暗号/復号化モジュール96の復号化ユニット111で、記憶モジュール92から供給された配送鍵 $K_d$ を用いて復号化する。次に、暗号処理部65の制御部91は、ステップS225で入力された個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ を、暗号/復号化モジュール96の復号化ユニット111で、個別鍵 $K_i$ を用いて復号化する。そして、暗号処理部65の制御部91は、暗号/復号化モジュール96の暗号化ユニット112で、ステップS220の相互認証時に据置機器52と共有した一時鍵 $K_{temp}$ を用いてコンテンツ鍵 $K_{co}$ を再暗号化する。ステップS229において、暗号処理部65の制御部91は、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ と、ステップS226で生成した使用許諾条件情報に対し、暗号/復号化モジ

ール96の署名生成ユニット114を用いて署名を生成し、上位コントローラ62に送信する。一時鍵K<sub>temp</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>、使用許諾条件情報およびそれらの署名を受信したホームサーバ51の上位コントローラ62は、大容量記憶部68からコンテンツ鍵K<sub>co</sub>で暗号化されたコンテンツ（署名を含む。以下同じ）を読み出し、一時鍵K<sub>temp</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>、使用許諾条件情報、それらの署名およびコンテンツ鍵K<sub>co</sub>で暗号化されたコンテンツを据置機器52に送信する。

#### 【0286】

ステップS230において、一時鍵K<sub>temp</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>、使用許諾条件情報、それらの署名およびコンテンツ鍵K<sub>co</sub>で暗号化されたコンテンツを受信した据置機器52は、署名を検証した後コンテンツ鍵K<sub>co</sub>で暗号化されたコンテンツを据置機器52の記録再生部76に出力する。コンテンツ鍵K<sub>co</sub>で暗号化されたコンテンツを受信した据置機器52の記録再生部76は、コンテンツ鍵K<sub>co</sub>で暗号化されたコンテンツを記録メディア80に保存する。

#### 【0287】

ステップS231において、据置機器52の暗号処理部73は、一時鍵K<sub>temp</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>を、暗号／復号化モジュールの復号化ユニットで、ステップS220の相互認証時にホームサーバ51と共有した一時鍵K<sub>temp</sub>を用いて復号化する。そして、暗号処理部73の制御部は、暗号／復号化モジュールの暗号化ユニットで、暗号処理部73の記憶モジュールから供給された保存鍵K<sub>save</sub>2を用いてコンテンツ鍵K<sub>co</sub>を再暗号化する。

#### 【0288】

ステップS232において、据置機器52の暗号処理部73は、保存鍵K<sub>save</sub>2で暗号化されたコンテンツ鍵K<sub>co</sub>とステップS230で受信した使用許諾条件情報を暗号処理部73の外部メモリ制御部に送信し、外部メモリ79に保存させる。外部メモリ制御部が外部メモリにデータを書き込む処理については、図69で説明しているので、詳細は省略する。

#### 【0289】

このように、ホームサーバ51はコンテンツ利用権を購入し、課金情報はホー

ムサーバ51側で保存し、利用権は据置機器52に引き渡される。

#### 【0290】

図75は、ホームサーバ51が、既に購入済みのコンテンツ利用権を、別の利用形態に変更して購入するための処理を示したフローチャートである。図75のステップS240からステップS245までは、図67で説明した処理と同様であるため、その説明は省略する。ステップS246において、ホームサーバ51の暗号処理部65は、暗号処理部65の外部メモリ制御部97に、利用権変更するコンテンツの使用許諾条件情報を読み出させる。外部メモリ67からのデータの読み出しは、図68を参照して説明したので、その詳細は省略する。ステップS246で正常に使用許諾条件情報が読み出せた場合には、ステップS247へ進む。

#### 【0291】

ステップS247において、ホームサーバ51の上位コントローラ62は、表示手段64を用いて利用権内容変更可能なコンテンツの情報（例えば、利用権内容変更可能な利用形態や価格など）を表示し、ユーザは入力手段63を用いて利用権内容更新条件を選択する。入力手段63から入力された信号はホームサーバ51の上位コントローラ62に送信され、上位コントローラ62は、その信号に基づいて利用権内容変更コマンドを生成し、利用権内容変更コマンドをホームサーバ51の暗号処理部65に入力する。これを受信した暗号処理部65は、ステップS243で受信した取扱方針、ステップS245で受信した価格情報およびステップS247で読み出した使用許諾条件情報から、課金情報および新しい使用許諾条件情報を生成する。

#### 【0292】

ステップS248は、図67のステップS171と同様なため、その詳細な説明は省略する。ステップS249において、暗号処理部65の制御部91は、ステップS247で生成した使用許諾条件情報を、暗号処理部65の外部メモリ制御部97に出力する。外部メモリ制御部97は、受信した使用許諾条件情報を外部メモリ67に上書き更新する。外部メモリ制御部97の外部メモリ67への書き換え（更新）方法は、図70で説明したので、その詳細は省略する。

## 【0293】

ステップS246において、外部メモリ67に、権利内容変更コマンドに付加されたコンテンツIDに対応する使用許諾条件情報が見つからなかった場合、または、使用許諾条件情報が記憶されている外部メモリの記憶ブロックに改竄が発見された場合（図68を参照して説明済み）、ステップS251へ進み、所定のエラー処理を行う。

## 【0294】

このように、ホームサーバ51は、既に購入した権利（使用許諾権条件情報に記述されている）と、取扱方針および価格情報を用いて新たな権利を購入し、利用権内容を変更することができる。

## 【0295】

図76及び図77は、取扱方針および価格情報のルール部分の具体例を示したものである。図76において、取扱方針は利用権ごとに整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータ、最低販売価格、コンテンツプロバイダの利益率から構成され、この取扱方針には例えば5つのルールが記述されている。ルール1は、権利項目が利用権内容番号1であるから、図44より、その権利は再生権、時間・回数制限なしの権利であることがわかる。また、パラメータの項目には、特に記述がないことがわかる。最低販売価格は¥350であり、コンテンツプロバイダ2の取り分は、価格の30%である。ルール2は、権利項目が利用権内容番号2であるから、図44より、その権利は再生権、時間制限有り、回数制限なしの権利であることがわかる。また、利用可能期間が1時間であることが、パラメータの項目からわかる。最低販売価格は¥100であり、コンテンツプロバイダ2の取り分は、価格の30%である。ルール3は、権利項目が利用権内容番号6であるから、図44より、その権利は複製権（コピー制御信号なし）、時間制限なし、回数制限ありの権利であることがわかる。また、利用可能回数が1回であることが、パラメータの項目からわかる。最低販売価格は¥30であり、コンテンツプロバイダ2の取り分は、価格の30%である。

## 【0296】

ルール4は、権利項目が利用権内容番号13であるから、図44より、その権利は利用内容変更であることがわかる。変更可能なルール番号は、#2（再生権、時間制限有り、回数制限なし）から#1（再生権、時間・回数制限なし）であることがパラメータの項目からわかる。最低販売価格は¥200であり、コンテンツプロバイダ2の取り分は、価格の20%である。最低販売価格がルール1より低く提示してあるのは、既に購入している権利を下取りして再購入すると考えているからであり、コンテンツプロバイダ2の取り分がルール1より低く提示してあるのは、実際の作業をする電子配信サービスセンタ1の取り分を増やすためである（コンテンツプロバイダ2は、権利内容変更時には作業がないため）。

## 【0297】

ルール5は、権利項目が利用権内容番号14であるから、図44より、その権利は再配布であることがわかる。再配布可能条件は、ルール番号#1（再生権、時間・回数制限なし）を持っている機器が、ルール番号#1（再生権、時間・回数制限なし）を購入して再配布することであることが、パラメータの項目からわかる。最低販売価格は¥250であり、コンテンツプロバイダ2の取り分は、価格の20%である。最低販売価格がルール1より低く提示してあるのは、既に購入している権利をもつ機器が、同一コンテンツにつき再購入すると考えているからであり、コンテンツプロバイダ2の取り分がルール1より低く提示してあるのは、実際の作業をする電子配信サービスセンタ1の取り分を増やすためである（コンテンツプロバイダ2は、再配付時には作業がないため）。

## 【0298】

図77において、価格情報は利用権ごとに整理番号として付けられたルール番号、パラメータ及び価格情報から構成され、この価格情報にも例えば5つのルールが記述されている。ルール1は、取扱方針のルール#1に対する価格情報で、利用権内容番号#1を購入する際に、価格が¥500で、サービスプロバイダ3の取り分が30%であることを示す。従って、ユーザが支払う¥500は、コンテンツプロバイダ2が¥150、サービスプロバイダ3が¥150、電子配信サービスセンタ1が¥200取ることになる。ルール2からルール5までも同様で

るので、その詳細は省略する。

#### 【0299】

なお、ルール4、5において、サービスプロバイダ2の取り分がルール1に比べて少ないので、サービスプロバイダ2の配信作業をユーザ機器が代行して行っており、代金の回収は電子配信サービスセンタ1が行っているためである。

#### 【0300】

また本例ではルール番号が#1から#5へと連番となっているが、必ずしもその必要はない。作成者はルール番号ごとに利用権内容番号とパラメータを設定しておき、そこから抽出したものを並べるため、一般には連番にならない。

#### 【0301】

図78は、図75で説明した権利内容変更を行う際の具体的な例を示したものである。取扱方針は利用権ごとに整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータ、最低販売価格、コンテンツプロバイダの利益率から構成され、価格情報は利用権ごとに整理番号として付けられたルール番号、パラメータ及び価格情報から構成され、使用許諾条件情報は利用権ごとに整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータから構成されている。ホームサーバ51は、既にルール番号#2の再生権、時間制限ありの権利を購入しており、権利内容を示す使用許諾条件情報には、ルール番号#2が記述されており、利用可能時間は残り30分で、今まで積算して2時間分の購入を行っていることを示している。今、時間制限ありから時間制限なしに変更しようとした場合、取扱方針のルール3、価格情報のルール3および使用許諾条件情報から¥200で再生権、時間・回数制限なしに変更でき、使用許諾条件情報は、ルール番号#1、利用権内容番号の再生権、時間・回数制限なしに変わることがわかる（利用権内容番号#1の場合のパラメータに関しては、後述する。また、本例で言えば、直接再生権、時間・回数制限なしを買う場合に比べ、一度、時間制限ありの権利を買ってから権利内容変更したほうが安くなってしまっている。このため、積算利用時間を見て割り引くようにした方がよい）。

## 【0302】

図79は、ホームサーバ51が据置機器52のために、コンテンツ利用権を購入し、その利用権を再配布する処理の詳細を説明したフローチャートである。ステップS260からステップ264は、図74のステップS220からステップS225と同様なため、その詳細な説明は省略する。ステップS265において、ホームサーバ51の暗号処理部65は、暗号処理部65の外部メモリ制御部97に、再配布しようとするコンテンツに対応する使用許諾条件情報および保存鍵K<sub>save</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>を、外部メモリ67から読み出させる。外部メモリ制御部97による外部メモリ67の読み出し方法については、図68で説明したので、その詳細は省略する。読み出しに成功した場合は、ステップS266に進む。

## 【0303】

ステップS266において、ホームサーバ51の上位コントローラ62は、表示手段64を用いて再配布可能なコンテンツの情報（例えば、再配布可能なコンテンツの利用形態や価格など）を表示し、ユーザは入力手段63を用いて再配付条件を選択する。なお、この選択処理は、予め再配付処理スタート時に行うようにしても良い。入力手段63から入力された信号はホームサーバ51の上位コントローラ62に送信され、上位コントローラ62は、その信号に基づいて再配布コマンドを生成し、再配布コマンドをホームサーバ51の暗号処理部65に入力する。これを受信した暗号処理部65は、ステップS264で受信した取扱方針、価格情報およびステップS265で読み出した使用許諾条件情報から、課金情報および新しい使用許諾条件情報を生成する。

## 【0304】

ステップS267は、図67のステップS171と同様なため、その詳細な説明は省略する。ステップS268において、暗号処理部65の制御部91は、ステップS265で読み出した保存鍵K<sub>save</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>を、暗号／復号化モジュール96の復号化ユニット111で、記憶モジュール92から供給された保存鍵K<sub>save</sub>を用いて復号化する。そして、暗号処理部65の制御部91は、暗号／復号化モジュール96の暗号化ユニット112で、ステップS

260の相互認証時に据置機器52と共有した一時鍵K<sub>temp</sub>を用いてコンテンツ鍵K<sub>co</sub>を再暗号化する。最後に、暗号／復号化モジュール96の署名生成ユニット114は、一時鍵K<sub>temp</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>と、ステップS266で生成した新しい使用許諾条件情報に対応した署名を生成し、暗号処理部65の制御部91に返送する。

#### 【0305】

ステップS269からステップS272の処理は、図74のステップS229からステップS232と同様なため、その詳細は省略する。

#### 【0306】

このように、ホームサーバ51は、自己の保持する利用権（使用許諾条件情報）と取扱方針、価格情報から新しい使用許諾条件情報を作り出し、自己の保持するコンテンツ鍵K<sub>co</sub>、コンテンツとともに据置機器52へ送信することで、コンテンツの再配布が行える。

#### 【0307】

図80は、ホームサーバ51が据置機器52のために、使用許諾条件情報、コンテンツ鍵K<sub>co</sub>を送信し、据置機器52でコンテンツ利用権を購入する処理の詳細を説明したフローチャートである。ステップS280において、据置機器52の暗号処理部73は、暗号処理部73の記憶モジュールに記憶されている課金情報の課金の合計が、上限に達しているか否か判定し、上限に達していなかった場合にはステップS281に進む（なお、課金合計上限で判定するのではなく、課金処理件数の上限で判定するようにしても良い）。

#### 【0308】

ステップS281において、据置機器52の上位コントローラ72は、据置機器52の小容量記憶部75から読み出した登録情報を据置機器52の暗号処理部73に入力する。登録情報を受信した暗号処理部73は、図示せぬ暗号／復号化モジュールの署名検証ユニットで登録情報の署名を検証した後、据置機器52のIDに対する「購入処理」の項目が「購入可」になっているか判定し、「購入可」であった場合にはステップS282に進む。

## 【0309】

ステップS282は、図74のステップS220と同様なため、その詳細は省略する。ステップS283は、図74のステップS221と同様なため、その詳細は省略する（ホームサーバ51は据置機器52が登録されているか否かを判定し、据置機器52はホームサーバ51が登録されているか否かを判定する）。ステップS284は、図79のステップS265と同様なため、その詳細は省略する。ステップS285は、図79のステップS268と同様なため、その詳細は省略する。ステップS286において、暗号処理部65の制御部91は、一時鍵K<sub>temp</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>と、ステップS284で読み出した使用許諾条件情報に対し、暗号／復号化モジュール96の署名生成ユニット114を用いて署名を生成し、上位コントローラ62に送信する。一時鍵K<sub>temp</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>、使用許諾条件情報およびそれらの署名を受信したホームサーバ51の上位コントローラ62は、大容量記憶部68からコンテンツ鍵K<sub>co</sub>で暗号化されたコンテンツ、必要に応じて取扱方針とその署名、価格情報との署名を読み出し、一時鍵K<sub>temp</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>、使用許諾条件情報、それらの署名、コンテンツ鍵K<sub>co</sub>で暗号化されたコンテンツ、取扱方針とその署名および価格情報とその署名を据置機器52に送信する。

## 【0310】

ステップS287は、図74のステップS230と同様なため、その詳細は省略する。ステップS288は、図74のステップS225と同様なため、その詳細は省略する。ステップS289において、据置機器52の上位コントローラ72は、表示手段78を用いて再配布可能なコンテンツの情報（例えば、再配布可能なコンテンツの利用形態や価格など）を表示し、ユーザは入力手段77を用いて再配付条件を選択する。なお、この選択処理は予め再配付処理スタート時に行うようにしても良い。入力手段77から入力された信号は据置機器52の上位コントローラ72に送信され、上位コントローラ72は、その信号に基づいて再配布コマンドを生成し、再配布コマンドを据置機器52の暗号処理部73に入力する。これを受信した暗号処理部73は、ステップS286で受信した取扱方針、価格情報および使用許諾条件情報から、課金情報および新しい使用許諾条件情報

を生成する。

#### 【0311】

ステップS290において、据置機器52の暗号処理部73は、ステップS289で生成した課金情報を図示せぬ暗号処理部73の記憶モジュールに保存する。ステップS291において、据置機器52の暗号処理部73は、ステップS286で受信した一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ を、図示せぬ暗号処理部73の復号化ユニットで、ステップS282で共有した一時鍵 $K_{temp}$ を用いて復号化する。そして、据置機器52の暗号処理部73は、図示せぬ暗号処理部73の暗号化ユニットで、図示せぬ暗号処理部73の記憶モジュールから供給された保存鍵 $K_{save}^2$ を用いてコンテンツ鍵 $K_{co}$ を暗号化する。

#### 【0312】

ステップS292において、据置機器52の暗号処理部73は、ステップS289で生成した使用許諾条件情報およびステップS291で生成した保存鍵 $K_{save}^2$ で暗号化されたコンテンツ鍵 $K_{co}$ を図示せぬ、暗号処理部73の外部メモリ制御部に送信する。使用許諾条件情報および保存鍵 $K_{save}^2$ で暗号化されたコンテンツ鍵 $K_{co}$ を受信した外部メモリ制御部は、使用許諾条件情報および保存鍵 $K_{save}^2$ で暗号化されたコンテンツ鍵 $K_{co}$ を外部メモリ79に書き込む。書き込む際の改竄チェックについては、図69を用いて説明したので、その詳細は省略する。

#### 【0313】

このように、据置機器52は、ホームサーバ51の保持する利用権（使用許諾条件情報）、取扱方針、価格情報、コンテンツ鍵 $K_{co}$ 、コンテンツをホームサーバ51から受信し、据置機器52で新しい使用許諾条件情報を作り出すことにより、コンテンツの再配布を受けることができる。

#### 【0314】

図81は、管理移動権について説明した図である。管理移動とは、機器1から機器2へ再生権を移動できる動作のことと、機器1から機器2へ権利が移動することは通常の移動と同じであるが、機器2は受け取った再生権を再移動することができない点で通常の移動と異なる（通常の移動と同様に、再生権を移動した後

の機器1は、再生権の再移動できない）。再生権を管理移動で受け取った機器2は、再生権を機器1に返還することができ、返還された後は、機器1は再度再生権の移動ができる、機器2は引き続きできない。これらを実現するため、使用許諾条件情報に管理移動権の購入者および現在の管理移動権の保持者を管理させてい（ここでは、利用権内容番号#1を持っている場合にのみ管理移動できることを想定しているが、利用権内容番号#2においても拡張できる）。

### 【0315】

図81において、取扱方針のルール1は、図78で説明しているので、その詳細は省略する。ルール2は、権利項目が利用権内容番号16であるから、図44より、その権利は管理移動権であることがわかる。また、パラメータの項目には、特に記述がないことがわかる。最低販売価格は¥100であり、コンテンツプロバイダ2の取り分は、価格の50%である。コンテンツプロバイダ2の取り分がルール1より高く提示してあるのは、サービスプロバイダ3は実際の作業を全く行わないため、その分をコンテンツプロバイダ2への取り分に回したためである。

### 【0316】

図81において、価格情報のルール1は、図78で説明しているので、その詳細は省略する。ルール2は、取扱方針のルール#2に対する価格情報で、利用権内容番号#16を購入する際に、価格が¥100で、サービスプロバイダ3の取り分が0%であることを示す。従って、ユーザが支払う¥100は、コンテンツプロバイダ2が¥50、サービスプロバイダ3が¥0、電子配信サービスセンター1が¥50取ることになる。

### 【0317】

図81において、ユーザはまずルール番号#1（再生権、時間・回数制限無し）を購入する。ただし、このとき管理移動権は持っていない（図81の(a)の状態）。次に、ユーザは管理移動権を購入する（これらの動作は一瞬なため、ユーザは一括して購入したように見える）。使用許諾条件のルール番号は、購入者を示す暗号処理部のID（以下購入者とする）がID1（例えば、ホームサーバ51のID）、再生権を保有する暗号処理部のID（以下保持者とする）がID

2になる(図81の(b)の状態)。これを、管理移動を行って据置機器52に移した場合、ホームサーバ51の持つ使用許諾条件情報のルール部は、購入者はID1のままだが、保持者がID2に変化する。また、管理移動により再生権を受信した据置機器52の持つ使用許諾条件情報のルール部は、購入者はID1、保持者はID2となり、ホームサーバ51の使用許諾条件情報と一緒にになっている。

### 【0318】

図82は、管理移動権の移動処理の詳細を説明するフローチャートである。図82において、ステップS300は、図74のステップS220と同様なため、その詳細は省略する。また、ステップS301は図74のステップS221と同様なため、その詳細は省略する。ステップS302は図75のステップS246と同様であため、その詳細は省略する。ステップS303において、ホームサーバ51の暗号処理部65は、読み出した使用許諾条件情報内のルール部を検査し、使用権が再生権、時間・回数制限なし、管理移動権ありになっているか判定する。管理移動権があると判定された場合、ステップS304に進む。

### 【0319】

ステップS304において、暗号処理部65の制御部91は、管理移動権の購入者および保持者が、共にホームサーバ51のIDになっているか判定する。管理移動権の購入者および保持者が、共にホームサーバ51のIDになっていると判定された場合には、ステップS305に進む。ステップS305において、暗号処理部65の制御部91は、使用許諾条件情報の管理移動権の保持者を据置機器52のIDに書き換える。ステップS306において、暗号処理部65の制御部91は、ステップS305で書き換えた使用許諾条件情報を暗号処理部65の外部メモリ制御部97に出力する。使用許諾条件情報を受信した暗号処理部65の外部メモリ制御部97は、外部メモリ67に使用許諾条件情報を上書き保存する。外部メモリ67のデータを書き換え保存する方法については、図70で説明したので、その詳細は省略する。ステップS307からステップS311までは、図79のステップS268からステップS272と同様なため、その詳細は省略する。

## 【0320】

ステップS303で使用許諾条件情報に管理移動権が含まれていなかった場合、ステップS304で管理移動権の購入者または保持者がホームサーバ51でなかった場合は、処理を中断する。

## 【0321】

このように、ホームサーバ51から据置機器52にコンテンツを再生するための権利を移動することができる。

## 【0322】

図83は、現在管理移動権を所持している据置機器52から、管理移動権の購入者であるホームサーバ51に、管理移動権を返還させる処理について説明したフローチャートである。図83において、ステップS320は、図74のステップS220と同様なため、その詳細は省略する。ステップS321は図74のステップS221と同様であため、その詳細は省略するが、ホームサーバ51と据置機器52双方で相手のIDが登録されているか検査しているものとする。登録されていると判定された場合、ステップS322に進む。ステップS322は、図75のステップS246と同様であるため、その詳細は省略するが、ホームサーバ51と据置機器52双方で同一のコンテンツIDのデータを読み出していることとする。外部メモリからデータが正しく読めた場合には、ステップS323に進む。ステップS323は、図82のステップS303と同様であるため、その詳細は省略するが、ホームサーバ51と据置機器52双方で管理移動権があるか判定していることとする。管理移動権があると判定された場合には、ステップS324に進む。

## 【0323】

ステップS324において、ホームサーバ51の暗号処理部65は、管理移動権の購入者がホームサーバ51のIDになっていて、保持者が据置機器52のIDになっているか判定する。管理移動権の購入者がホームサーバ51のIDになっていて、保持者が据置機器52のIDになっていると判定された場合には、ステップS325に進む。同様に、据置機器52の暗号処理部73は、管理移動権の購入者がホームサーバ51のIDになっていて、保持者が据置機器52のID

になっているか判定する。管理移動権の購入者がホームサーバ51のIDになっていて、保持者が据置機器52のIDになっていると判定された場合には、ステップS325に進む。

#### 【0324】

ステップS325において、据置機器52の記録再生部76は、記録メディア80からコンテンツを削除する（ただし、暗号化されたデータが残るだけなので、無理に削除する必要はない）。ステップS326において、据置機器52の暗号処理部73は、図示せぬ暗号処理部73の外部メモリ制御部に、外部メモリ79に保存されている保存鍵K<sub>save</sub>2で暗号化されたコンテンツ鍵K<sub>co</sub>と使用許諾条件情報を削除させる。外部メモリ79の照りの削除方法は図71で説明したので、その詳細は省略する。

#### 【0325】

ステップS327において、暗号処理部65の制御部91は、使用許諾条件情報の管理移動権の保持者をホームサーバ51のIDに書き換えた使用許諾条件情報を生成する。ステップS328において、暗号処理部65の制御部91は、ステップS327で生成した使用許諾条件情報を、暗号処理部65の外部メモリ制御部97に出力する。使用許諾条件情報を受信した暗号処理部65の外部メモリ制御部97は、外部メモリ67に使用許諾条件情報を上書き保存する。外部メモリ67に書き換え保存する方法については、図70で説明したので、その詳細は省略する。

#### 【0326】

ステップS321でホームサーバ51または据置機器52において、登録情報が改竄されていたり、相手の機器のIDが登録されていなかった場合、ステップS322でホームサーバ51または据置機器52において、外部メモリ内に所定のコンテンツに対するコンテンツ鍵または使用許諾条件情報が見つからなかったり、それらを含むメモリブロックが改竄されていた場合は、ステップS329へ進みエラー処理を行う。

#### 【0327】

ステップS323でホームサーバ51または据置機器52において、使用許諾

条件情報内に管理移動権がなかった場合、ステップS324でホームサーバ51または据置機器52において、購入者がホームサーバ51で、保持者が据置機器52でなかった場合は、処理を中断する。

#### 【0328】

このように、据置機器52からホームサーバ51にコンテンツを再生するための権利をもどすことができる。

#### 【0329】

なお、コンテンツおよびコンテンツ鍵K<sub>co</sub>等を1つしか記述していないが、必要に応じて複数存在することとする。

#### 【0330】

また、本例ではコンテンツプロバイダ2とサービスプロバイダ3が別々に扱われていたが、一つにまとめてしまってもよい。更にまた、コンテンツプロバイダ2の方式を、そのままサービスプロバイダ3に転用しても良い。

#### 【0331】

##### (2) 個別鍵の使用による暗号化処理

コンテンツプロバイダ2は、図9について上述したようにコンテンツを自ら作成したコンテンツ鍵で暗号化する。また、コンテンツプロバイダ2は、電子配信サービスセンタ1からコンテンツプロバイダ固有の個別鍵と、配送鍵で暗号化された個別鍵を受け取り、個別鍵によってコンテンツ鍵を暗号化する。かくしてコンテンツプロバイダ2は、コンテンツ鍵で暗号化されたコンテンツと、個別鍵で暗号化されたコンテンツ鍵と、配送鍵で暗号化された個別鍵とをサービスプロバイダ3を介してユーザホームネットワーク5に供給する。

#### 【0332】

ユーザホームネットワーク5では、電子配信サービスセンタ1から受け取った配送鍵を用いてコンテンツプロバイダ固有の個別鍵を復号化する。これにより、ユーザホームネットワーク5はコンテンツプロバイダ2からコンテンツプロバイダ固有の個別鍵で暗号化されて供給されるコンテンツ鍵を復号することができる。コンテンツ鍵を得たユーザホームネットワーク5は当該コンテンツ鍵によりコンテンツを復号することができる。

## 【0333】

ここで、個別鍵はコンテンツサーバごとに固有であるのに対して、配送鍵は一種類のみである。従って、ユーザホームネットワーク5は一種類の配送鍵だけを持っていれば、各コンテンツプロバイダからの個別鍵を復号することができる。従って、ユーザホームネットワーク5は各コンテンツプロバイダ固有の個別鍵を持つ必要がなくなり、配送鍵を持つだけですべてのコンテンツプロバイダのコンテンツを購入することができる。

## 【0334】

また、各コンテンツプロバイダは、配送鍵を持たないことにより、他のコンテンツプロバイダ固有の個別鍵（配送鍵で暗号化されている）を復号することができない。これによりコンテンツプロバイダ間でのコンテンツの盗用を防止し得る。

## 【0335】

ここで、以上の実施の形態の構成と、特許請求の範囲に記載の発明の各手段とを明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

## 【0336】

すなわち、本発明の情報送信システムにおいては、コンテンツ等の情報を送信するコンテンツ供給者又はコンテンツ販売業者（例えば、図84のコンテンツ送信装置200）が持つ個別鍵保存用メモリ（例えば、図84の耐タンパメモリ201）、コンテンツ鍵K<sub>co</sub>を個別鍵K<sub>i</sub>で暗号化するための手段（例えば、図84のデータ暗号部203）、コンテンツ鍵K<sub>co</sub>の使用条件等を記述した取扱方針を生成するための手段（例えば、図84の取扱方針生成部206）、各種データに対してディジタル署名を生成するための手段（例えば、図84の署名生成部207）と、コンテンツを購入するユーザ（例えば、図84のコンテンツ受信装置210）が持つ各種データに対して生成された署名データを検証する手段（例えば、図84の署名検証部222）、コンテンツ鍵K<sub>co</sub>の生成者を示すIDと取扱方針の生成者のIDとを比較するための手段（例えば、図84の比較器226）

、配送鍵を保存するための手段（例えば、図84の耐タンパメモリ221）とを備える。

### 【0337】

また、本発明の情報送信システムにおいては、コンテンツ等の情報を送信するコンテンツ供給者又はコンテンツ販売業者（例えば、図85のコンテンツ送信装置200）が持つ個別鍵保存用メモリ（例えば、図85の耐タンパメモリ201）、鍵証明書を保存するためのメモリ（例えば、図85のメモリ202）、コンテンツ鍵 $K_{co}$ を個別鍵 $K_i$ で暗号化するための手段（例えば、図85のデータ暗号部203）、コンテンツを購入するユーザ（例えば、図85のコンテンツ受信装置210）が持つ各種データに対して生成された署名データを検証する手段（例えば、図85の署名検証部222）、配送鍵を保存するための手段（例えば、図85の耐タンパメモリ221）とを備える。

### 【0338】

#### （3）遠隔再生処理

コンテンツの再生権利を保持していない機器（例えば据置機器52）でコンテンツを保持している機器（例えばホームサーバ51）から再生コマンドを受け取り、コンテンツを再生する遠隔再生処理について説明する。

### 【0339】

図86は遠隔再生処理手順を示し、まず、ユーザの入力操作によって遠隔再生しようとするコンテンツのコンテンツIDが上位コントローラ62に入力された後、ステップS401において、ホームサーバ51と据置機器52は相互認証する。相互認証処理は、図52で説明した処理と同様であるため、説明を省略する。ステップS402において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した登録情報を、ホームサーバ51の暗号処理部65に検査させる。上位コントローラ62から登録情報を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115に、登録情報に付加されている署名を、暗号処理部65の記憶モジュール92から供給された認証局22の公開鍵で検証させる。署名の検証に成功した後、「登録」の項目が「登録可」になっているか判定し、「登録可」になっていると判定さ

れた場合にはステップS403に進む。なお、据置機器52側でも登録情報を検査し、ホームサーバ51が「登録可」になっていることを判定している。

#### 【0340】

ステップS403において上位コントローラ62は遠隔再生しようとするコンテンツのコンテンツIDを含む再生コマンドを生成し、続くステップS404において、ホームサーバ51の暗号処理部65は、暗号処理部65の外部メモリ制御部97に、遠隔再生しようとするコンテンツに対応する使用許諾条件情報及び保存鍵K<sub>save</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>を、外部メモリ67から読み出させる。外部メモリ制御部97による外部メモリ67からのデータ読み出し方法については、図68で説明した通りであり、その詳細は省略する。読み出しに成功した場合、ステップS405に進む。

#### 【0341】

ステップS405において、暗号／復号化モジュール96の復号化ユニット111は、外部メモリ67から読み出したコンテンツ鍵K<sub>co</sub>を、記憶モジュール92から供給された保存鍵K<sub>save</sub>で復号化する。ステップS406において、暗号／復号化モジュール96の暗号化ユニット112は、一時鍵K<sub>temp</sub>でコンテンツ鍵K<sub>co</sub>を暗号化した後、ステップS407において再生コマンドを一時鍵K<sub>temp</sub>で暗号化する。

#### 【0342】

ホームサーバ51は続くステップS408において、遠隔再生しようとするコンテンツ（コンテンツ鍵K<sub>co</sub>で暗号化されている）を大容量記憶部68から読み出して、これを上述のステップS406及びS407において一時鍵K<sub>temp</sub>で暗号化されたコンテンツ鍵及び再生コマンドと共に据置機器52に送信する。

#### 【0343】

ステップS409において、据置機器52はホームサーバ51から受け取ったコンテンツ鍵及び再生コマンドを一時鍵K<sub>temp</sub>で復号化し、ステップS410において暗号処理部73と伸張部74は相互認証を行い、一時鍵K<sub>temp</sub>2を共有する。そしてステップS411において暗号処理部73は上述のステップS410において伸張部74と共有した一時鍵K<sub>temp</sub>2でコンテンツ鍵K<sub>co</sub>及び再生コマ

ンドを暗号化する。ステップS412において、暗号処理部73は一時鍵K<sub>temp</sub>2で暗号化されたコンテンツ鍵K<sub>co</sub>及び再生コマンドを伸張部74に送信し、伸張部74はステップS413においてコンテンツ鍵K<sub>co</sub>及び再生コマンドを一時鍵K<sub>temp</sub>2で復号化する。

#### 【0344】

伸張部74はステップS414において、ホームサーバ51から上述のステップS408においてホームサーバ51から受け取ったコンテンツを上述のステップS413において復号化された再生コマンドに従って上述のステップS413において復号化されたコンテンツ鍵K<sub>co</sub>で復号化する。そして伸張部74は当該復号化されたコンテンツをステップS415において所定の方式、例えばA T R A Cなどの方式により伸張する。ステップS416において、上位コントローラ72は暗号処理部73から指示されたデータを電子透かしの形でコンテンツに挿入する。因みに、暗号処理部73から伸張部74へ渡されるデータは、コンテンツ鍵K<sub>co</sub>及び再生コマンドだけではなく、再生条件（アナログ出力、ディジタル出力、コピー制御信号付き出力（SCMS））、コンテンツ利用権を購入した機器IDなども含まれている。挿入するデータは、このコンテンツ利用権を購入した機器のID、つまりは、使用許諾条件情報内の機器IDなどである。ステップS417において、伸張部74は、図示せぬスピーカを介して音楽を再生する。

#### 【0345】

以上の構成において、ホームサーバ51はコンテンツと当該コンテンツの再生コマンド及びコンテンツ鍵K<sub>co</sub>を据置機器52に送信することにより、コンテンツの再生権利を保持していない据置機器52は、再生コマンド及びコンテンツ鍵K<sub>co</sub>を用いてコンテンツを再生することができる。従って、以上の構成によれば、コンテンツを保持する機器（コンテンツの再生権利を有する機器）に接続された複数の機器（据置機器等）において、コンテンツを再生することができる。

#### 【0346】

##### （4）予約購入処理

配送鍵の有効期限が切れる前にコンテンツの鍵変換を予め行っておき、コンテンツの購入予約を行うホームサーバの予約購入処理について説明する。図87に

示す予約購入処理手順のステップS451において、ホームサーバ51は登録情報更新判断処理を行い、ステップS452に進む。登録情報更新判断処理については、図61及び図62で説明した通りであり、その詳細説明は省略する。但し、予約購入処理においては、図61のステップS601やS602で述べた購入個数や購入金額に基づく登録情報更新タイミングの判断は行わなくても良い。

#### 【0347】

ステップS452において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した登録情報をホームサーバ51の暗号処理部65に入力する。登録情報を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で登録情報の署名を検証した後、ホームサーバ51のIDに対する「購入処理」及び「登録」の項目が「購入可」及び「登録可」になっているか否かを判定し、「購入可」及び「登録可」であった場合にはステップS453に進む。ステップS453において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツプロバイダ2の公開鍵証明書をホームサーバ51の暗号処理部65に入力する。コンテンツプロバイダ2の公開鍵証明書を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツプロバイダ2の公開鍵証明書の署名を検証した後、公開鍵証明書からコンテンツプロバイダ2の公開鍵を取り出す。署名の検証の結果、改ざんがなされていないことが確認された場合には、上位コントローラ62はステップS454に進む。

#### 【0348】

ステップS454においてホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツ鍵K<sub>c0</sub>をホームサーバ51の暗号処理部65に入力する。コンテンツ鍵K<sub>c0</sub>を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツ鍵K<sub>c0</sub>の署名を検証し、改ざんがなされていないことが確認された場合には、ステップS455に進む。

#### 【0349】

ステップS455において、ホームサーバ51の上位コントローラ62は、ホ

ームサーバ51の大容量記憶部68から読み出した個別鍵K<sub>i</sub>をホームサーバ51の暗号処理部65に入力する。個別鍵K<sub>i</sub>を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で個別鍵K<sub>i</sub>の署名を検証し、改ざんがなされていないことが確認された場合には、ステップS456に進む。

#### 【0350】

ここで、個別鍵K<sub>i</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>及び配送鍵K<sub>d</sub>で暗号化された個別鍵K<sub>i</sub>全体に対して1つの署名がついている場合は、S454及びS455を1つに合わせることができ署名検証処理を簡略化できる。

#### 【0351】

ステップS456において、暗号処理部65の制御部91は、ステップS455で入力された個別鍵K<sub>i</sub>を、暗号／復号化モジュール96の復号化ユニット111で、記憶モジュール92から供給された配送鍵K<sub>d</sub>を用いて復号化する。次に、暗号処理部65の制御部91は、ステップS454で入力されたコンテンツ鍵K<sub>co</sub>を、暗号／復号化モジュール96の復号化ユニット111で、先ほど復号化した個別鍵K<sub>i</sub>を用いて復号化する。最後に、暗号処理部65の制御部91は、暗号／復号化モジュール96の暗号化ユニット112で、記憶モジュール92から供給された保存鍵K<sub>save</sub>を用いてコンテンツ鍵K<sub>co</sub>を暗号化する。

#### 【0352】

ステップS457において、保存鍵K<sub>save</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>は、暗号処理部65の外部メモリ制御部97を経由して外部メモリ67に保存される。

#### 【0353】

また、ステップS452でホームサーバ51が購入処理できない機器であると判定された場合、又はステップS453でコンテンツプロバイダ2の公開鍵証明書の署名が正しくないと判定された場合、又はステップS454で個別鍵K<sub>i</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>の署名が正しくないと判定された場合、又はステップS455で配送鍵K<sub>d</sub>で暗号化された個別鍵K<sub>i</sub>の署名が正しくないと判定された場合、ホームサーバ51はステップS458に進み、エラー処理を行う。

## 【0354】

以上のように、ホームサーバ51は、コンテンツ鍵K<sub>co</sub>を個別鍵K<sub>i</sub>で復号化した後、コンテンツ鍵K<sub>co</sub>を保存鍵K<sub>save</sub>で再暗号化し、外部メモリ67に記憶させる。この予約購入処理は、実際にコンテンツを購入しないので、図67について上述した購入処理のうち、ステップS161の登録情報更新判断処理のなかの課金情報についての処理、ステップS164に対応する購入コンテンツについての処理、ステップS167に対応する取扱い方針についての処理、ステップS168に対応するサービスプロバイダの公開鍵検証についての処理、ステップS169に対応する価格情報の署名検証についての処理、ステップS170乃至ステップS172に対応する課金情報及び使用許諾条件情報の保存処理は行わなくても良い。

## 【0355】

因みに、図87の予約購入処理の場合、ホームサーバ51は使用許諾条件情報の作成は行わなかったが、これに代えて使用許諾条件情報を作成しその利用権内容番号（すなわち権利項目）を初期値等の権利を持っていない状態（例えば、存在しない#0など）としておくようにしても良い。

## 【0356】

このようにして、予約購入処理では、ホームサーバ51は配送鍵K<sub>d</sub>の有効期限が切れる前にコンテンツ鍵K<sub>co</sub>を外部メモリ67に保存しておくことにより、当該保存されたコンテンツ鍵K<sub>co</sub>によって暗号化されたコンテンツについて、配送鍵K<sub>d</sub>の期限に関わらず購入することができる。

## 【0357】

ここで、ホームサーバ51において外部メモリ67にコンテンツ鍵K<sub>co</sub>を保存することにより購入の予約がなされたコンテンツの本購入処理について説明する。図83に示す本購入処理手順のステップS471において、ホームサーバ51は登録情報更新判断処理を行い、ステップS472に進む。登録情報更新判断処理については、図61及び図62で説明した通り、その詳細は、省略する。しかし、本購入処理においては、図61のステップS603で述べた配送鍵K<sub>d</sub>に基づく登録情報更新タイミングの判断は行わなくて良い。

## 【0358】

ステップS472において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した登録情報をホームサーバ51の暗号処理部65に入力する。登録情報を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で登録情報の署名を検証した後、ホームサーバ51のIDに対する「購入処理」及び「登録」の項目が「購入可」及び「登録可」になっているか判定し、「購入可」及び「登録可」であった場合にはステップS473に進む。ステップS473において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツプロバイダ2の公開鍵証明書をホームサーバ51の暗号処理部65に入力する。コンテンツプロバイダ2の公開鍵証明書を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツプロバイダ2の公開鍵証明書の署名を検証した後、公開鍵証明書からコンテンツプロバイダ2の公開鍵を取り出す。署名の検証の結果、改ざんがなされていないことが確認された場合には、ステップS474に進む。

## 【0359】

ステップS474において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツをホームサーバ51の暗号処理部65に入力する。コンテンツを受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツの署名を検証し、改ざんがなされていないことが確認された場合には、ステップS475に進む。

## 【0360】

ステップS475において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した取扱方針をホームサーバ51の暗号処理部65に入力する。取扱方針を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で取扱方針の署名を検証し、改ざんがなされていないことが確認された場合には、ステップS476に進む。ステップS476において、ホームサーバ51の上位コントローラ62は、ホームサ

ーバ51の大容量記憶部68から読み出したサービスプロバイダ3の公開鍵証明書をホームサーバ51の暗号処理部65に入力する。サービスプロバイダ3の公開鍵証明書を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でサービスプロバイダ3の公開鍵証明書の署名を検証した後、公開鍵証明書からサービスプロバイダ3の公開鍵を取り出す。署名の検証の結果、改ざんがなされていないことが確認された場合には、ステップS477に進む。

#### 【0361】

ステップS477において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した価格情報をホームサーバ51の暗号処理部65に入力する。価格情報を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で価格情報の署名を検証し、改ざんがなされていないことが確認された場合には、ステップS478に進む。

#### 【0362】

ステップS478において、ホームサーバ51の上位コントローラ62は、表示手段64を用いて購入可能なコンテンツの情報（例えば、購入可能な利用形態や価格など）を表示し、ユーザは入力手段63を用いて購入項目を選択する。なお、購入項目の選択処理は本購入処理に先立って行うようにしても良い。入力手段63から入力された信号はホームサーバ51の上位コントローラ62に送信され、上位コントローラ62は、その信号に基づいて購入コマンドを生成し、購入コマンドをホームサーバ51の暗号処理部65に入力する。これを受信した暗号処理部65は、ステップS475で入力された取扱方針及びステップS477で入力された価格情報から課金情報を生成する。課金情報については、図42で説明した通りであり、その詳細は省略する。また、使用許諾条件情報については、図41で説明した通りであり、その詳細は省略する。

#### 【0363】

ステップS479において、暗号処理部65の制御部91は、ステップS478で生成した課金情報を記憶モジュール92に保存する。そしてステップS480において、暗号処理部65の制御部91は、ステップS478で生成した使用

許諾条件情報を暗号処理部65の外部メモリ制御部97に送信する。使用許諾条件情報を受信した外部メモリ制御部97は、外部メモリ67の改ざんチェックを行った後、使用許諾条件情報を外部メモリ67に書き込む。書き込む際の改ざんチェックについては、図69について上述した通りであり、詳細説明は省略する（なお、権利なしの使用許諾条件情報がすでに書き込まれている場合には、図70で説明した書き換え処理により使用許諾条件情報を書き換え更新する）。

#### 【0364】

因みに、ステップS472でホームサーバ51が購入処理できない機器であったり、登録されていないと判定された場合、又はステップS473でコンテンツプロバイダ2の公開鍵証明書の署名が正しくないと判定された場合、又はステップS474でコンテンツ鍵K<sub>co</sub>で暗号化されたコンテンツの署名が正しくないと判定された場合、又はステップS475で取扱方針の署名が正しくないと判定された場合、又はステップS476でサービスプロバイダ3の公開鍵証明書の署名が正しくないと判定された場合、又はステップS477で価格情報の署名が正しくないと判定された場合、ホームサーバ51はステップS481に進み、エラー処理を行う。

#### 【0365】

以上のように、ホームサーバ51ではユーザが購入選択したコンテンツについての課金情報を記憶モジュール92に記憶すると共に、使用許諾条件情報を外部メモリ67に記憶することにより、コンテンツの本購入処理を終了する。この本購入処理では、図87について上述した予約購入処理で既に行われたコンテンツ鍵K<sub>co</sub>の署名検証（ステップS454）及び個別鍵K<sub>i</sub>の署名検証（ステップS455）、並びにコンテンツ鍵K<sub>co</sub>のかけ替え処理（ステップS456）は行わない。

#### 【0366】

以上の構成において、ホームサーバ51では配送鍵K<sub>d</sub>が更新される前に予約購入処理によりコンテンツ鍵K<sub>co</sub>を外部メモリ67に保存しておくことにより、コンテンツ鍵K<sub>co</sub>を復号化する際に必要となる配送鍵K<sub>d</sub>が更新されても、コンテンツ鍵K<sub>co</sub>は既に外部メモリ67に保存されているので、配送鍵K<sub>d</sub>の有効期

限が切れてもコンテンツを購入することができる。

### 【0367】

#### (5) 代理購入処理

登録情報(Registration List)が異なっている機器、すなわちグループが異なる機器間においてコンテンツの授受を行う代理購入処理について説明する。この代理購入処理では、例えばホームサーバ51と当該ホームサーバ51に対してグループ外機器である携帯機器等との間でコンテンツを授受する場合について、ホームサーバ51側で課金する場合と、グループ外機器で課金を行う場合をそれぞれ説明する。この場合、図15について上述した据置機器52をグループ外機器として説明する。

### 【0368】

図89はホームサーバ51がグループ外機器にコンテンツを渡し、ホームサーバ51が課金処理を行う場合の処理手順を示し、ステップS501において、ホームサーバ51とグループ外機器は、相互認証する。相互認証処理は、図52で説明した処理と同様であるため、説明を省略する。ステップS502において、ホームサーバ51とグループ外機器とは互いに登録情報を交換し、続くステップS503において互いに相手の登録情報を検査する。

### 【0369】

すなわち、ホームサーバ51はグループ外機器から受け取った登録情報を、暗号処理部65に検査させる。グループ外機器からの登録情報を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115に、登録情報に付加されている署名を、暗号処理部65の記憶モジュール92から供給された公開鍵で検証させる。署名の検証に成功した後、暗号処理部65の制御部91は、登録情報にグループ外機器のIDが登録され、「購入処理」及び「登録」の項目が「購入可」及び「登録可」になっているか否かを判定する。また、ホームサーバ51の登録情報を受け取ったグループ外機器も、同様にしてホームサーバ51の登録情報にホームサーバ51のIDが登録され、「登録」の項目が「登録可」になっているか否かを判定する。そして、互いに相手の機器が登録されていることが確認されると、ホームサーバ51はステップS504に移る。

## 【0370】

ステップS504からステップS510は、図67のステップS161からステップS171までと同様な処理なため、その詳細は省略する。

## 【0371】

ステップS511において、暗号処理部65の制御部91は、ステップS508で入力された配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を、暗号／復号化モジュール96の復号化ユニット111で、記憶モジュール92から供給された配送鍵 $K_d$ を用いて復号化する。次に、暗号処理部65の制御部91は、ステップS508で入力された個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ を、暗号／復号化モジュール96の復号化ユニット111で、先ほど復号化した個別鍵 $K_i$ を用いて復号化する。そして、暗号処理部65の制御部91は、暗号／復号化モジュール96の暗号化ユニット112で、ステップS501の相互認証時にグループ外機器と共有した一時鍵 $K_{temp}$ を用いてコンテンツ鍵 $K_{co}$ を再暗号化する。ステップS512において、暗号処理部65の制御部91は、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ と、ステップS509で生成した使用許諾条件情報に対し、暗号／復号化モジュール96の署名生成ユニット114を用いて署名を生成し、上位コントローラ62に送信する。一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報およびそれらの署名を受信したホームサーバ51の上位コントローラ62は、大容量記憶部68からコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを読み出し、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報、それらの署名およびコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツをグループ外機器に送信する。

## 【0372】

ステップS513において、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報、それらの署名およびコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを受信したグループ外機器は、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツをグループ外機器の記録再生部76に出力する。コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを受信したグループ外機器の記録再生部76は、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを記録メディア80に保存する。

## 【0373】

ステップS514において、グループ外機器の暗号処理部73は、上述のステップS512でホームサーバから受け取った署名の検証を行うと共に、一時鍵K<sub>temp</sub>で暗号化されたコンテンツ鍵K<sub>co</sub>を、暗号／復号化モジュールの復号化ユニットで、ステップS501の相互認証時にホームサーバ51と共有した一時鍵K<sub>temp</sub>を用いて復号化する。そして、暗号処理部73の制御部は、暗号／復号化モジュールの暗号化ユニットで、暗号処理部73の記憶モジュールから供給された保存鍵K<sub>save</sub>2を用いてコンテンツ鍵K<sub>co</sub>を再暗号化する。

## 【0374】

ステップS515において、グループ外機器の暗号処理部73は、保存鍵K<sub>sa</sub>ve2で暗号化されたコンテンツ鍵K<sub>co</sub>とステップS513で受信した使用許諾条件情報を暗号処理部73の外部メモリ制御部に送信し、外部メモリ79に保存させる。外部メモリ制御部が外部メモリにデータを書き込む処理については、図69で説明しているので、詳細は省略する。

## 【0375】

このように、ホームサーバ51はコンテンツ利用権を購入し、課金情報はホームサーバ51側で保存し、利用権はグループ外機器に引き渡される。これにより、ホームサーバ51はグループ外機器に引き渡したコンテンツ利用権についてその支払いを行うことになる。

## 【0376】

次に、図90はホームサーバ51がグループ外機器にコンテンツを渡し、グループ外機器が課金処理を行う場合の処理手順を示し、ステップS551においてグループ外機器は、暗号処理部73（図15）内に記憶されている課金情報の課金の合計が、上限に達しているか否か判定し、上限に達していなかった場合にはステップS552に進む（なお、課金合計上限で判定するのではなく、課金処理件数の上限で判定するようにしても良い）。

## 【0377】

ステップS552において、グループ外機器の上位コントローラ72は、外部メモリ79から読み出した登録情報を暗号処理部73に入力する。登録情報を受

信した暗号処理部73は、その内部に設けられた暗号／復号化モジュールの署名検証ユニットで登録情報の署名を検証した後、グループ外機器（据置機器52）のIDに対する「購入処理」の項目が「購入可」になっているか判定し、「購入可」であった場合にはステップS553に進む。

#### 【0378】

ステップS553において、ホームサーバ51とグループ外機器は、相互認証する。相互認証処理は、図52で説明した処理と同様であるため、説明を省略する。ステップS554において、ホームサーバ51とグループ外機器とは互いに登録情報を交換し、続くステップS555において互いに相手の登録情報を検査する。

#### 【0379】

すなわち、ホームサーバ51はグループ外機器から受け取った登録情報を、暗号処理部65に検査させる。グループ外機器からの登録情報を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115に、登録情報に付加されている署名を、暗号処理部65の記憶モジュール92から供給された公開鍵で検証させる。署名の検証に成功した後、暗号処理部65の制御部91は、登録情報にグループ外機器のIDが登録され、「登録」の項目が「登録可」になっているか否かを判定する。また、ホームサーバ51の登録情報を受け取ったグループ外機器も、同様にしてホームサーバ51の登録情報にホームサーバ51のIDが登録され、「登録」の項目が「登録可」になっているか否かを判定する。なお、同様の処理をグループ外機器も行っている。そして、互いに相手の機器が登録されていることが確認されると、ホームサーバ51はステップS556に移る。

#### 【0380】

ステップS556において、ホームサーバ51の制御部91は、外部メモリ制御部97を介して外部メモリ67から既に購入済のコンテンツ鍵を読み出し、続くステップS557においてコンテンツ鍵K<sub>co</sub>を保存鍵K<sub>save</sub>で復号化すると共に一時鍵K<sub>temp</sub>で再暗号化し、それらの署名を生成する。

## 【0381】

ステップS558において、ホームサーバ51は、S557で生成した保存鍵K<sub>temp</sub>で暗号化されたコンテンツ鍵と大容量記憶部68から読みだしたコンテンツ、取扱方針、価格情報をグループ外機器に送信する。ステップS559においてグループ外機器は、ホームサーバ51から受け取ったコンテンツを記録メディア80に保存する。

## 【0382】

ステップS560において、グループ外機器（据置機器52）は取扱方針、価格情報等の署名を検証した後、ステップS561において、グループ外機器の上位コントローラ72は、表示手段78を用いて購入可能なコンテンツの情報（例えば、購入可能な利用形態や価格など）を表示し、ユーザは入力手段77を用いて購入項目を選択する。なお購入項目の選択処理は代理購入処理に先立って行うようにしても良い。入力手段77から入力された信号は上位コントローラ72に送信され、上位コントローラ72は、その信号に基づいて購入コマンドを生成し、購入コマンドを暗号処理部73に入力する。これを受信した暗号処理部73は、ステップS560で入力された取扱方針および価格情報から課金情報および使用許諾条件情報を生成する。課金情報については、図42で説明したので、その詳細は省略する。使用許諾条件情報については、図41で説明したので、その詳細は省略する。

## 【0383】

ステップS562において、暗号処理部73は、ステップS561で生成した課金情報を暗号処理部73内の記憶モジュールに保存する。ステップS563において、暗号処理部73は、ステップS557で暗号化されたコンテンツ鍵について、署名を検証すると共に一時鍵K<sub>temp</sub>で復号化し、保存鍵K<sub>save</sub>2で再暗号化する。そしてステップS564において、保存鍵K<sub>save</sub>2で暗号化されたコンテンツ鍵K<sub>co</sub>は、暗号処理部73から外部メモリ79に保存される。

## 【0384】

このように、ホームサーバ51は既に購入したコンテンツ利用権をグループ外機器に引き渡し、グループ外機器は課金情報も保存することにより、グループ外

機器はグループ外のホームサーバ51から引き渡されたコンテンツ利用権についてその支払いを行うことになる。

#### 【0385】

以上の構成において、登録情報(Registration List)が異なっている機器間ににおいて、上述のステップS502及びステップS554について上述したように、互いの登録情報を交換することにより、登録された機器であることを確認した後一方の機器が有するコンテンツを他方の機器に引き渡すことができる。従って、以上の構成によれば、グループが異なる機器間においてコンテンツの授受を行うことができる。

#### 【0386】

なお、上述の実施の形態においては、購入処理の際にコンテンツの署名を検証したが、処理に時間がかかるため省略する場合がある。また、取扱方針又は価格情報に、検証の必要性の有無を記述し、それに従つて動作する場合がある。

#### 【0387】

##### 【発明の効果】

上述のように本発明によれば、コンテンツを再生する権利を保持していない機器においても、コンテンツを保持している機器から再生コマンドを受け取り、コンテンツを再生することができる。

##### 【図面の簡単な説明】

###### 【図1】

本発明による電子音楽配信システムの全体構成を示すブロック図である。

###### 【図2】

電子配信サービスセンタの構成を示すブロック図である。

###### 【図3】

鍵の定期的な更新例を示す略線図である。

###### 【図4】

鍵の定期的な更新例を示す略線図である。

###### 【図5】

鍵の定期的な更新例を示す略線図である。

【図6】

鍵の定期的な更新例を示す略線図である。

【図7】

ユーザ登録データベースのデータ内容を示す略線図である。

【図8】

グループごとの登録情報を示す略線図である。

【図9】

コンテンツプロバイダの構成を示すブロック図である。

【図10】

署名生成処理手順を示すフローチャートである。

【図11】

署名検証処理手順を示すフローチャートである。

【図12】

楕円曲線暗号化方法を示すフローチャートである。

【図13】

楕円曲線暗号化の復号化処理を示すフローチャートである。

【図14】

サービスプロバイダの構成を示すブロック図である。

【図15】

ユーザホームネットワークの構成を示すブロック図である。

【図16】

外部メモリ制御部の動作の説明に供する略線図である。

【図17】

電子配信専用記録メディアの構成を示すブロック図である。

【図18】

各機器の持つデータ内容を示すブロック図である。

【図19】

記録メディアが保持するデータ内容を示すブロック図である。

【図20】

システム全体のデータの流れを示す略線的ブロック図である。

【図21】

公開鍵証明書の流れを示す略線的ブロック図である。

【図22】

コンテンツプロバイダセキュアコンテナを示す略線図である。

【図23】

コンテンツプロバイダセキュアコンテナを示す略線図である。

【図24】

コンテンツプロバイダセキュアコンテナを示す略線図である。

【図25】

コンテンツプロバイダセキュアコンテナを示す略線図である。

【図26】

コンテンツプロバイダの公開鍵証明書を示す略線図である。

【図27】

コンテンツプロバイダの公開鍵証明書を示す略線図である。

【図28】

コンテンツプロバイダの公開鍵証明書を示す略線図である。

【図29】

サービスプロバイダセキュアコンテナを示す略線図である。

【図30】

サービスプロバイダセキュアコンテナを示す略線図である。

【図31】

サービスプロバイダの公開鍵証明書を示す略線図である。

【図32】

ユーザ機器の公開鍵証明書を示す略線図である。

【図33】

シングルコンテンツの取扱方針を示す略線図である。

【図34】

アルバムコンテンツの取扱方針を示す略線図である。

【図35】

シングルコンテンツの取扱方針の他の例を示す略線図である。

【図36】

アルバムコンテンツの取扱方針の他の例を示す略線図である。

【図37】

シングルコンテンツの価格情報を示す略線図である。

【図38】

アルバムコンテンツの価格情報を示す略線図である。

【図39】

シングルコンテンツの価格情報の他の例を示す略線図である。

【図40】

アルバムコンテンツの価格情報の他の例を示す略線図である。

【図41】

使用許諾条件情報を示す略線図である。

【図42】

課金情報を示す略線図である。

【図43】

課金情報の他の例を示す略線図である。

【図44】

利用権内容の一覧を示す略線図である。

【図45】

利用権を示す略線図である。

【図46】

シングルコンテンツを示す略線図である。

【図47】

アルバムコンテンツを示す略線図である。

【図48】

シングルコンテンツ用の鍵データを示す略線図である。

【図49】

個別鍵の暗号化処理の説明に供するブロック図である。

【図50】

アルバムコンテンツ用の鍵データを示す略線図である。

【図51】

対称鍵技術を用いた相互認証処理を示すタイミングチャートである。

【図52】

非対称鍵暗号技術を用いた相互認証処理を示すタイミングチャートである。

【図53】

課金情報の送信動作を示す略線的ブロック図である。

【図54】

利益分配処理動作を示す略線的ブロック図である。

【図55】

コンテンツ利用実績の送信動作を示す略線的ブロック図である。

【図56】

コンテンツの配布及び再生処理手順を示すフローチャートである。

【図57】

コンテンツプロバイダへの送信処理手順を示すフローチャートである。

【図58】

決済情報の登録処理手順を示すフローチャートである。

【図59】

機器IDの新規登録処理手順を示すフローチャートである。

【図60】

機器の追加登録処理手順を示すフローチャートである。

【図61】

登録情報の更新開始条件の判断処理を示すフローチャートである。

【図62】

登録情報更新処理手順を示すフローチャートである。

【図63】

据置機器による登録情報更新代理処理手順を示すフローチャートである。

【図64】

据置機器による登録情報更新代理処理手順を示すフローチャートである。

【図65】

セキュアコンテナの送信処理手順を示すフローチャートである。

【図66】

セキュアコンテナの送信処理手順を示すフローチャートである。

【図67】

ホームサーバの購入処理手順を示すフローチャートである。

【図68】

データ読み出し時の改竄チェック処理手順を示すフローチャートである。

【図69】

データ書き込み時の改竄チェック処理手順を示すフローチャートである。

【図70】

データ書換え時の改竄チェック処理手順を示すフローチャートである。

【図71】

データ削除時の改竄チェック処理手順を示すフローチャートである。

【図72】

ホームサーバによるコンテンツの再生処理手順を示すフローチャートである。

【図73】

ホームサーバによるコンテンツの再生処理手順を示すフローチャートである。

【図74】

ホームサーバによるコンテンツ利用権の代理購入処理手順を示すフローチャートである。

【図75】

購入済利用者の内容変更処理手順を示すフローチャートである。

【図76】

取扱方針のルール部の内容を示す略線図である。

【図77】

価格情報のルール部の内容を示す略線図である。

【図78】

権利内容の変更例を示す略線図である。

【図79】

コンテンツ利用権の再配布処理手順を示すフローチャートである。

【図80】

据置機器でのコンテンツ利用権購入処理手順を示すフローチャートである。

【図81】

使用許諾条件情報のルール部の変遷を示す略線図である。

【図82】

管理移動権の移動処理手順を示すフローチャートである。

【図83】

管理移動権の返還処理手順を示すフローチャートである。

【図84】

本発明による情報送信システムを示すブロック図である。

【図85】

本発明による情報送信システムを示すブロック図である。

【図86】

遠隔再生処理手順を示すフローチャートである。

【図87】

予約購入処理手順を示すフローチャートである。

【図88】

予約購入後の本購入処理手順を示すフローチャートである。

【図89】

ホームサーバが課金する場合の代理購入処理手順を示すフローチャートである

【図90】

グループ外機器が課金する場合の代理購入処理手順を示すフローチャートである。

【図91】

従来例を示すブロック図である。

【符号の説明】

1 ……電子配信サービスセンタ、 2 ……コンテンツプロバイダ、 3 ……サービスプロバイダ、 4 ……ネットワーク、 5 ……ユーザホームネットワーク、 10 ……電子音楽配信システム、 11 ……サービスプロバイダ管理部、 12 ……コンテンツプロバイダ管理部、 13 ……著作権管理部、 14 ……鍵サーバ、 15 ……経歴データ管理部、 16 ……利益分配部、 17 ……相互認証部、 18 ……ユーザ管理部、 19 ……課金請求部、 20 ……出納部、 21 ……監査部、 22 ……認証局、 23 ……コンテンツサーバ、 24 ……コンテンツオーサリング部、 31 ……コンテンツサーバ、 32 ……電子透かし付加部、 34 ……コンテンツ暗号部、 35 ……コンテンツ鍵生成部、 36 ……コンテンツ鍵暗号部、 37 ……取扱方針生成部、 38 ……署名生成部、 39 ……相互認証部、 41 ……コンテンツサーバ、 42 ……証明書検証部、 43 ……署名検証部、 44 ……値付け部、 45 ……署名生成部、 46 ……相互認証部、 51 ……ホームサーバ、 52 ……据置機器、 53 ……携帯機器、 62、 72、 82 ……上位コントローラ、 65、 73、 83 ……暗号処理部、 66、 74、 84 ……伸張部、 67、 79、 85 ……外部メモリ、 120 ……電子配信専用記録メディア。

【書類名】図面

【図1】

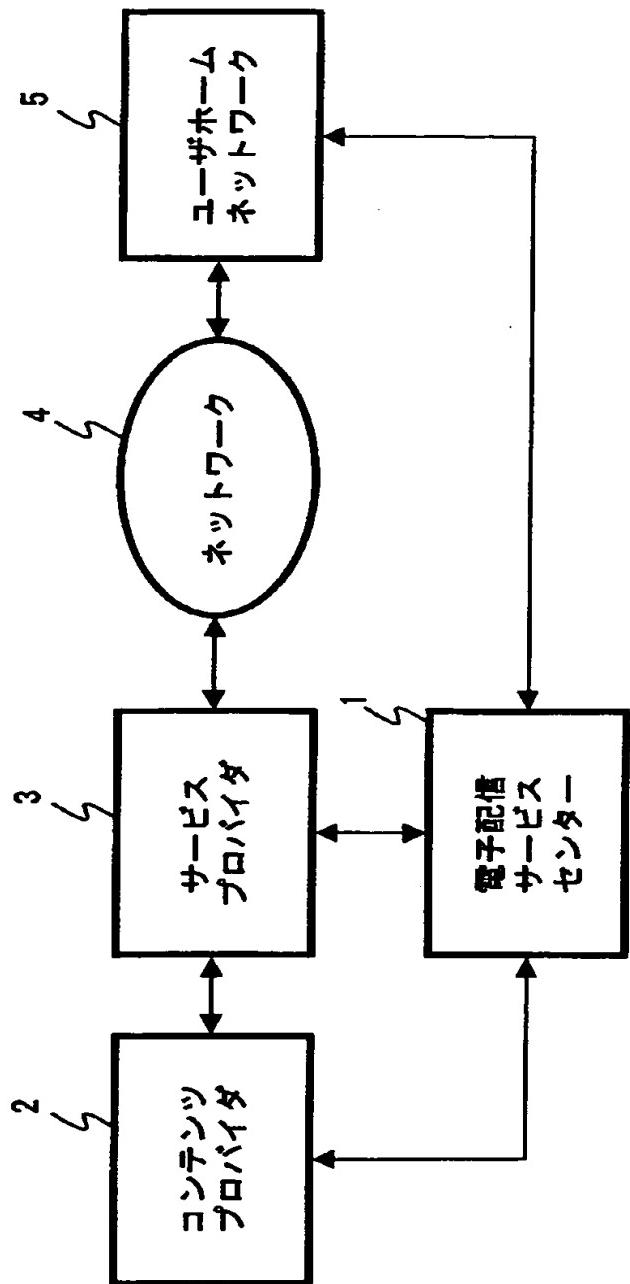


図1 電子音楽配信システムの全体構成

【図2】

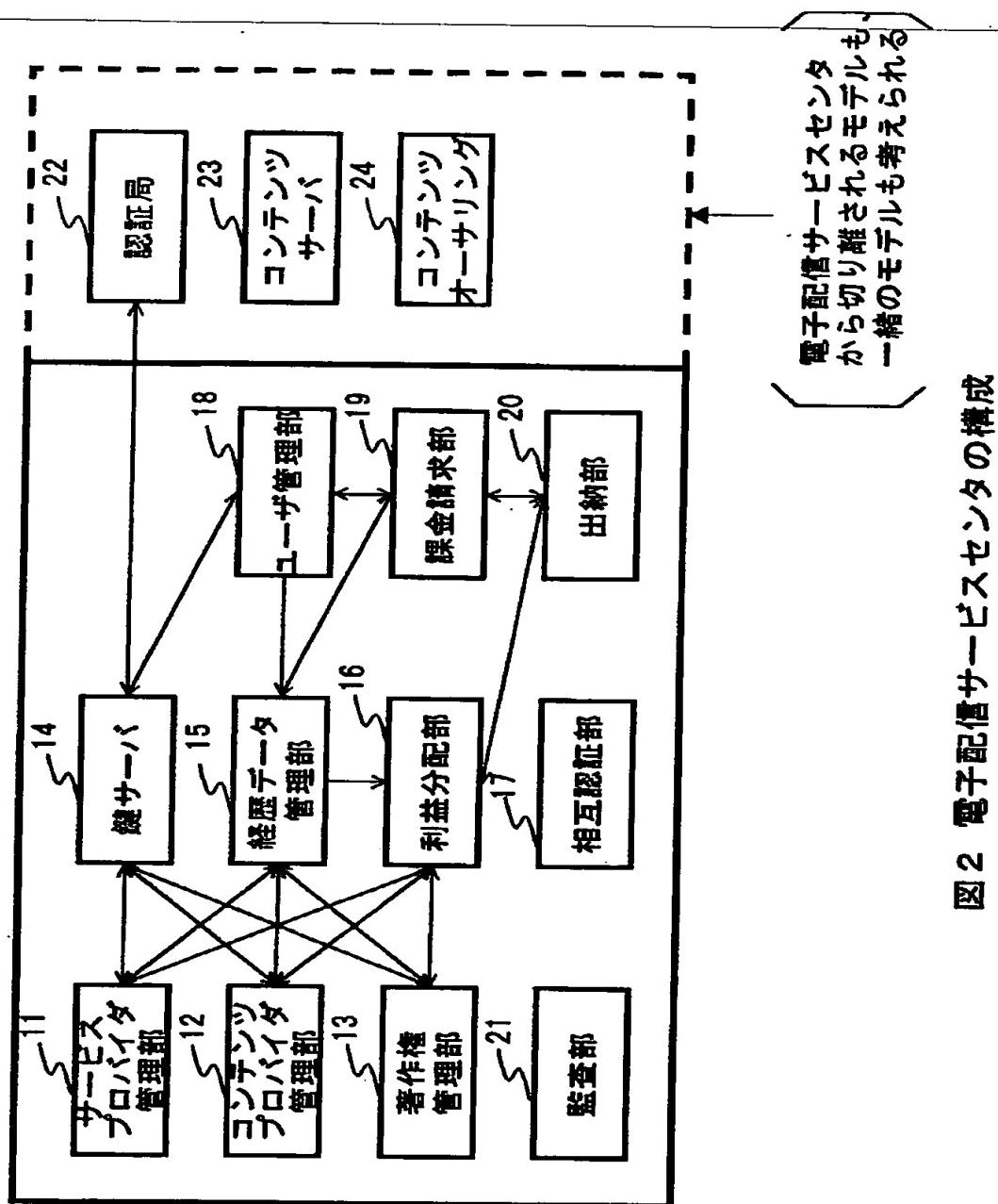


図2 電子配信サービスセントラルの構成

電子配信サービスセントラルから切り離されるモデルも、一緒にモデルも考えられる

【図3】

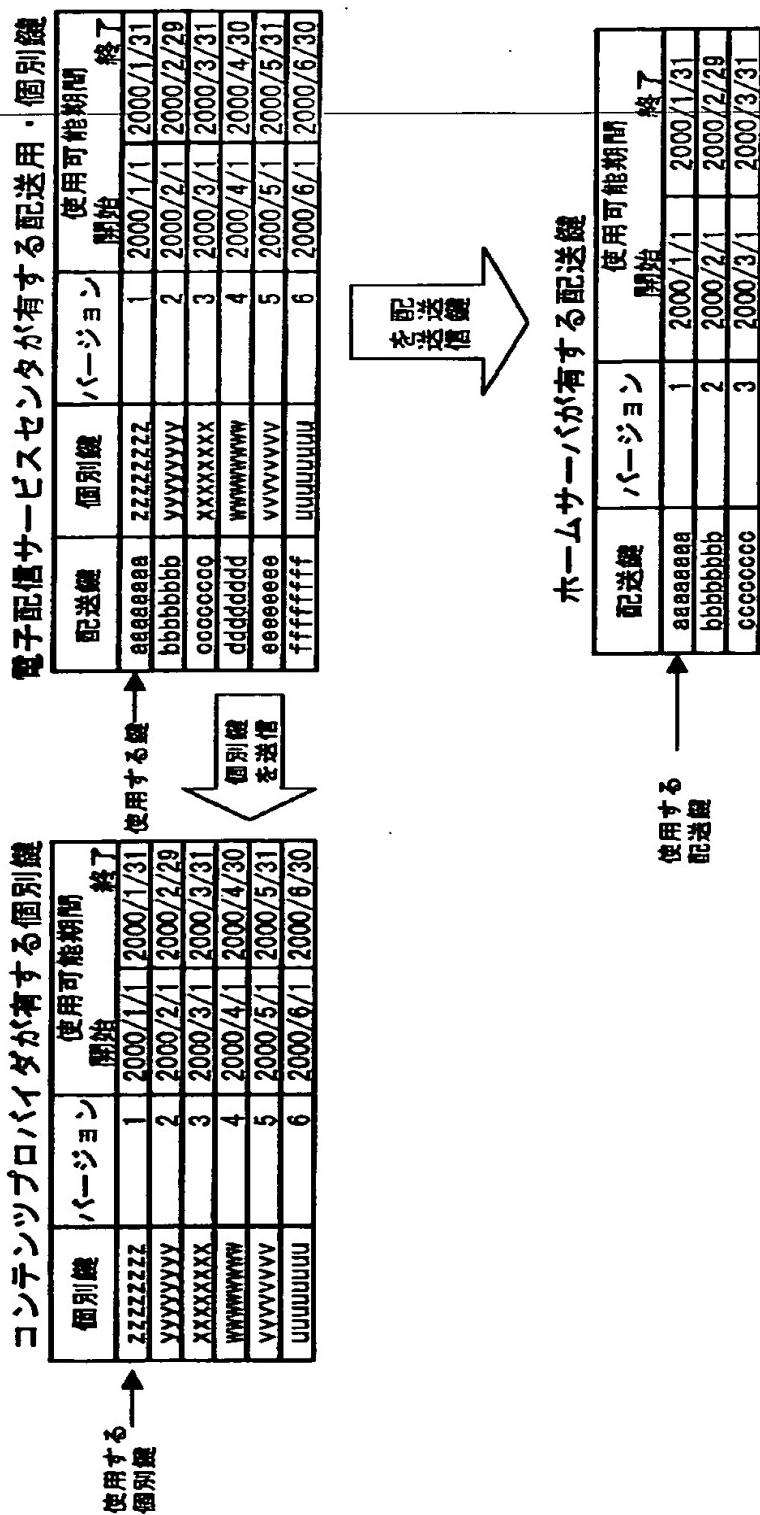


図3 鍵の定期的な送信例(1)

### 【図4】

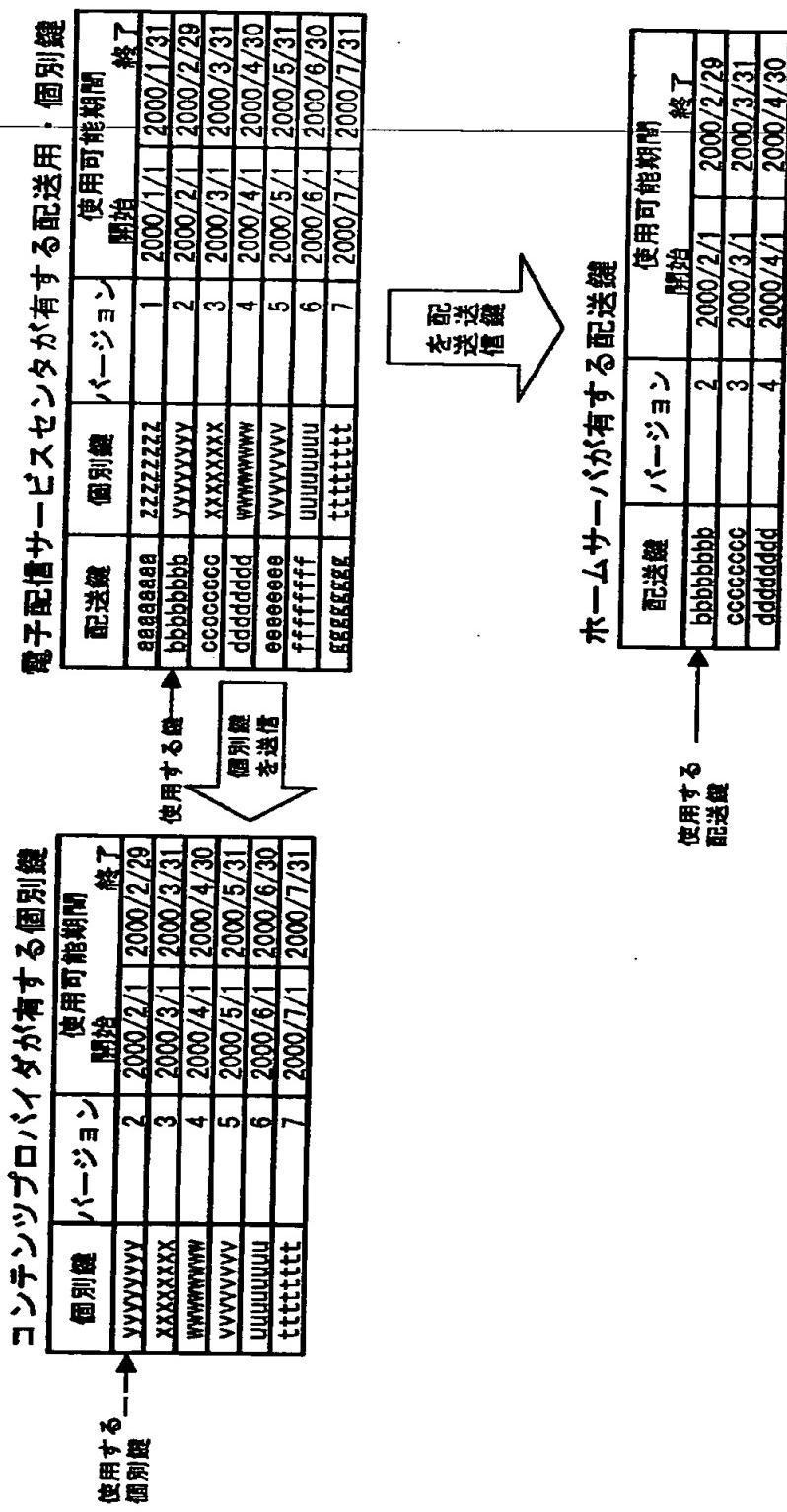


図4 鍵の定期的な送信例 (2)

【図5】

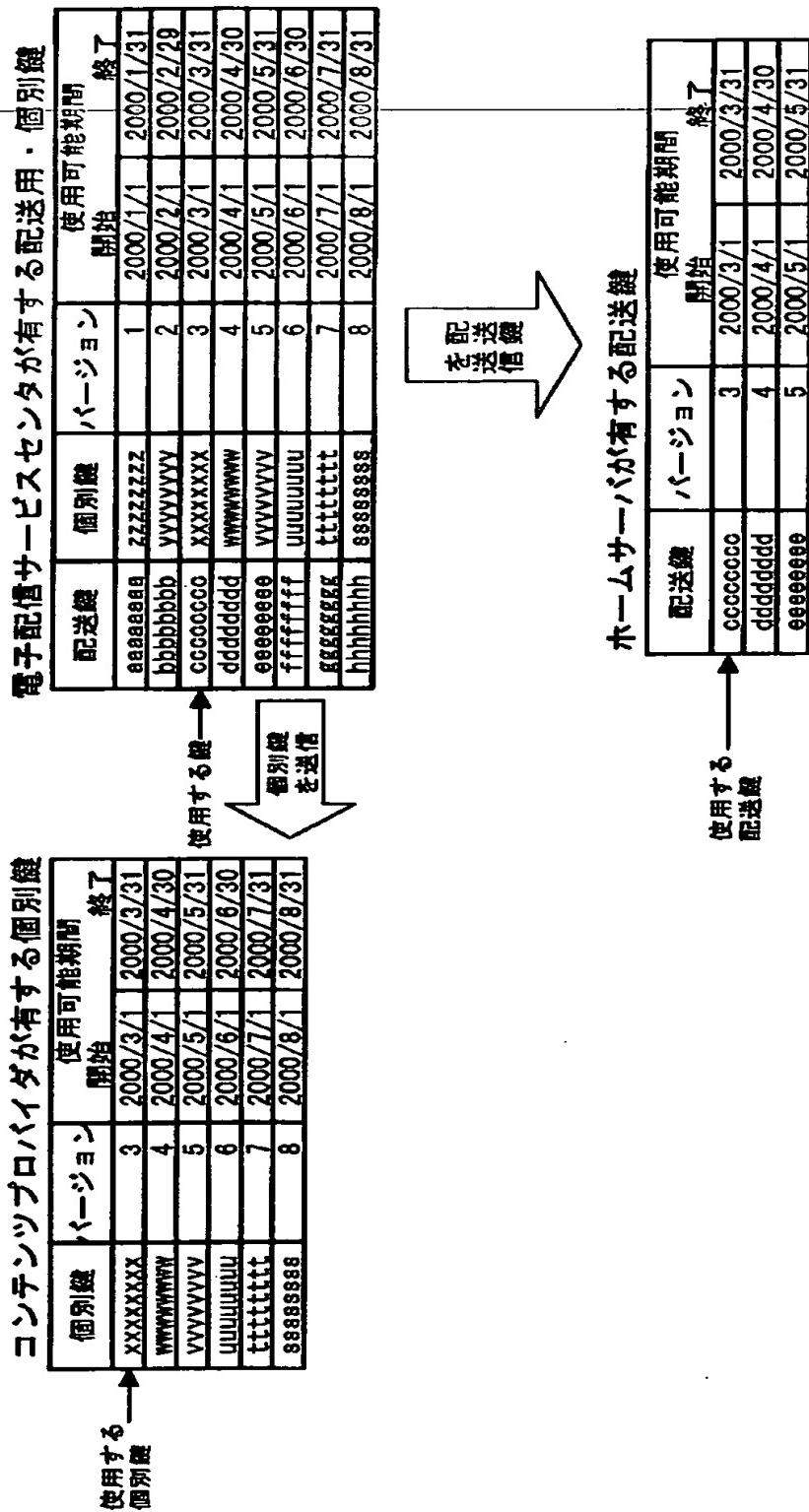


図5 鍵の定期的な送信例（3）

【図 6】

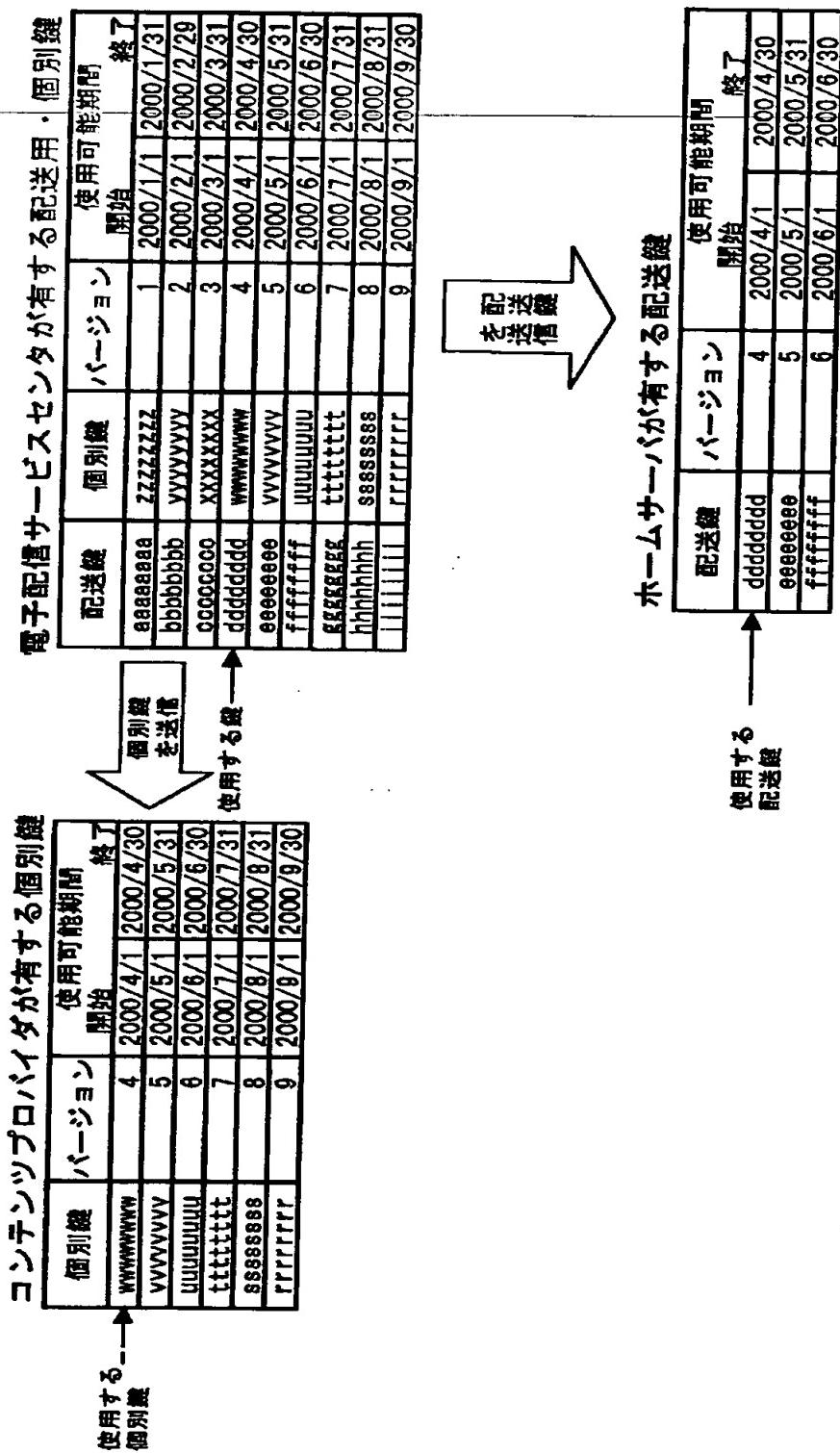


図 6 鍵の定期的な送信例（4）

【図7】

グループID	ID	サービスセントとの接続	決済処理	購入処理	代理購入者	登録
GpID1	ID1	可	可	可	-	可
	ID2	可	不可	可	ID1	可
	ID3	可	不可	可	ID1	可
	ID4	不可	不可	不可	-	不可
	ID5	不可	不可	不可	-	可
GpID2	ID6	可	可	可	-	不可
	ID7	可	不可	可	-	不可
	ID8	可	不可	可	ID6	可
	ID9	不可	不可	不可	-	不可
	ID10	不可	不可	不可	-	可
GpID3	ID11	可	可	可	-	不可
	ID12	可	不可	可	ID11	不可
	ID13	可	不可	可	ID11	可
	ID14	不可	不可	不可	-	可
	ID15	不可	不可	不可	-	可

図7 ユーザ登録データベース

【図8】

		ID	サービスセンタとの接続	決済処理	決済ID	購入処理	代理決済者	代理購入者	登録	署名
		グルーブID	サービスセンタとの接続	決済処理	決済ID	購入処理	代理決済者	代理購入者	登録	署名
(A)	Q1D1	ID1	可	可	決済ID1	可	—	—	可	可
	Q1D2	ID2	可	不可	—	可	ID1	—	可	可
	Q1D3	ID3	可	不可	—	可	ID1	—	不可	署名
	Q1D4	ID4	不可	不可	—	不可	—	ID1	可	可
	Q1D5	ID5	不可	不可	—	不可	—	ID2	不可	不可

		ID	サービスセンタとの接続	決済処理	決済ID	購入処理	代理決済者	代理購入者	登録	署名
		グルーブID	サービスセンタとの接続	決済処理	決済ID	購入処理	代理決済者	代理購入者	登録	署名
(B)	Q1D2	ID6	可	可	決済ID2	可	—	—	可	可
	Q1D3	ID7	可	不可	—	可	ID6	—	可	可
	Q1D4	ID8	可	不可	—	可	ID6	—	不可	署名
	Q1D5	ID9	不可	不可	—	不可	—	ID6,7,8	可	可
	Q1D6	ID10	不可	不可	—	不可	—	ID6,7,8	不可	不可

図8 グループの登録情報

【図9】

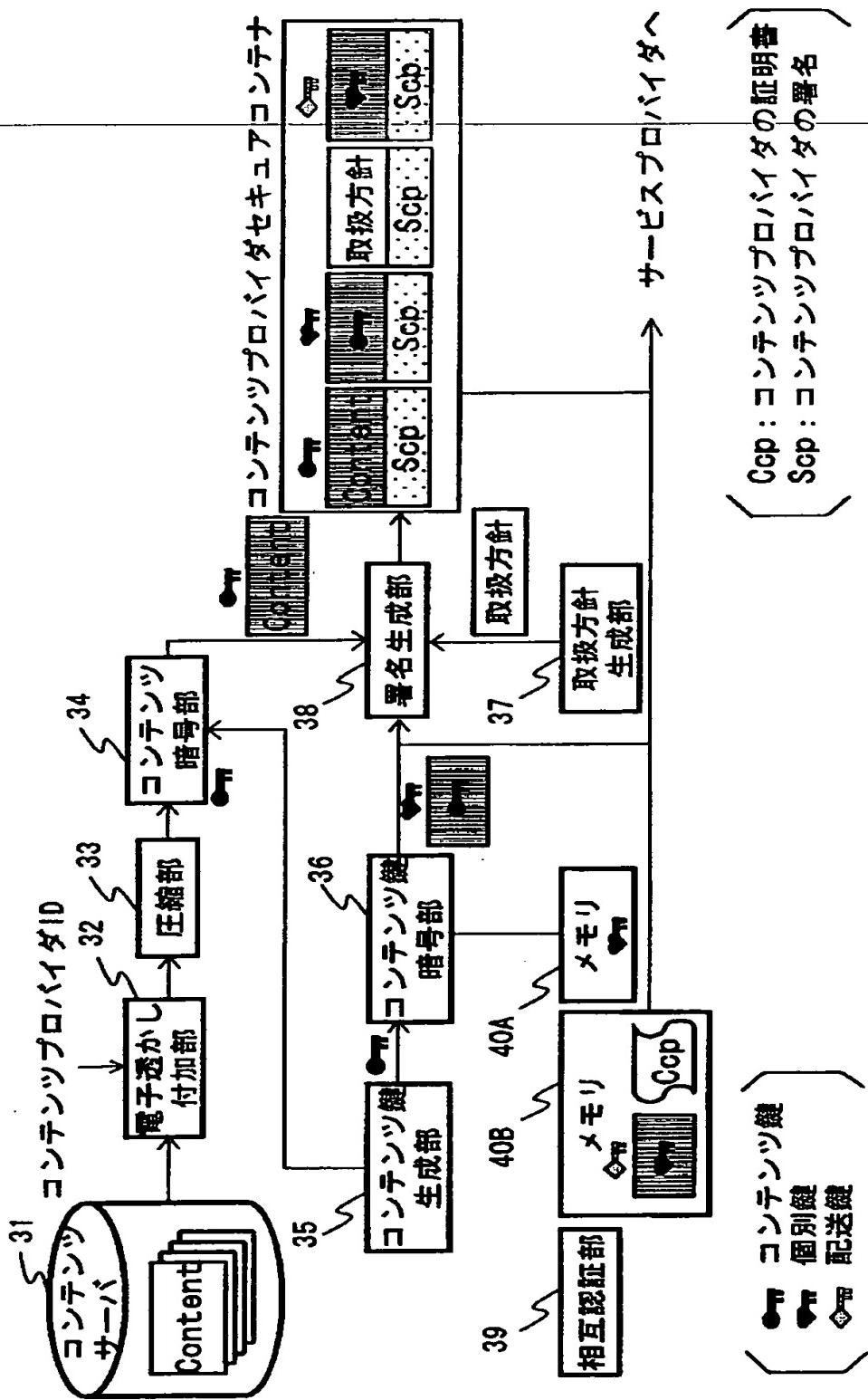


図9 コンテンツプロバイダの構成

【図10】

## (署名生成)

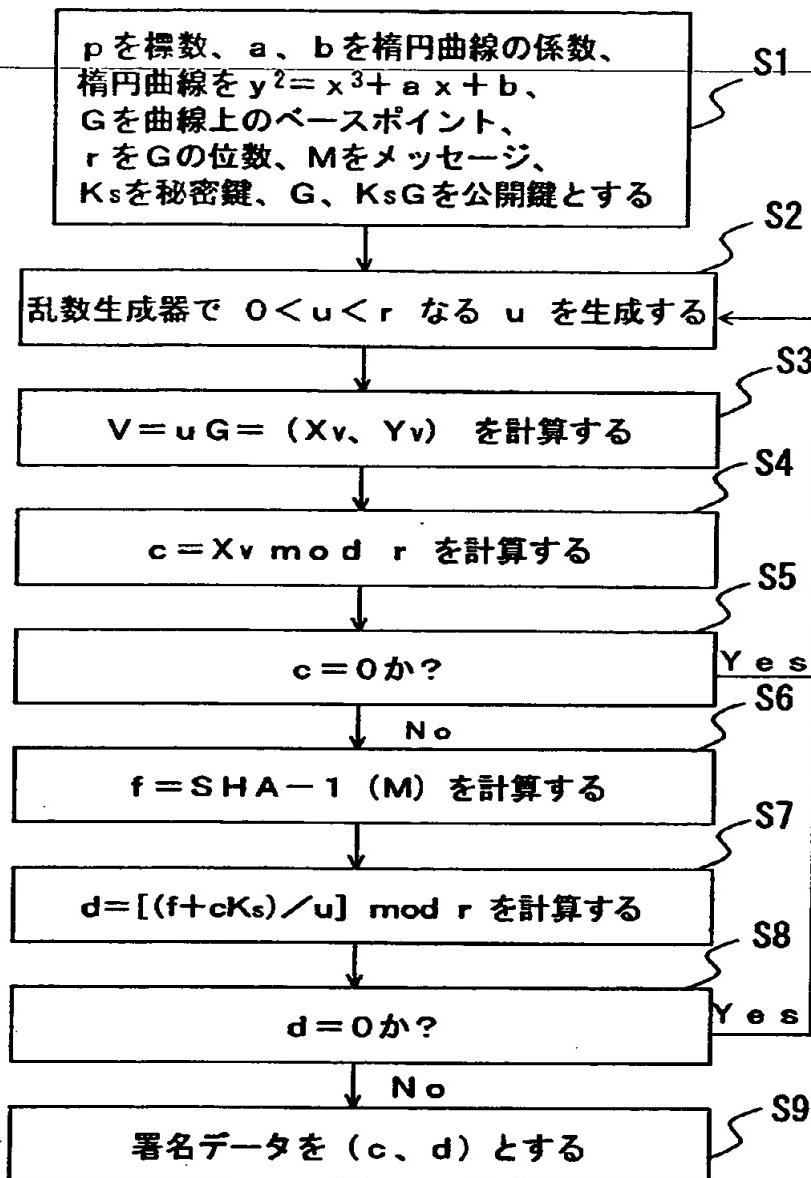


図10 署名生成 (IEEE P1363/D3) 处理

【図11】

## (署名検証)

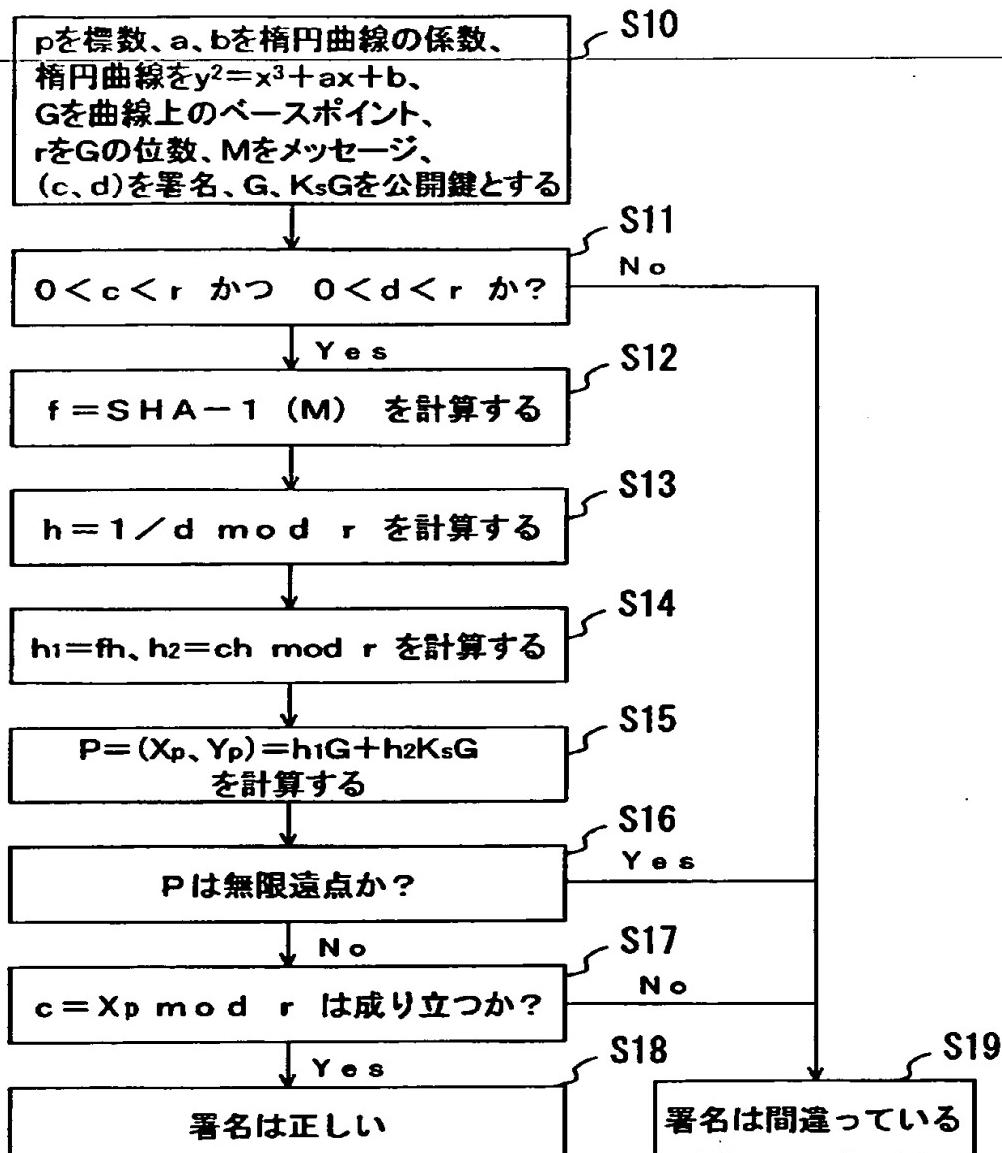


図11 署名検証 (IEEE P1363/D3) 処理

【図12】

## (暗号化)

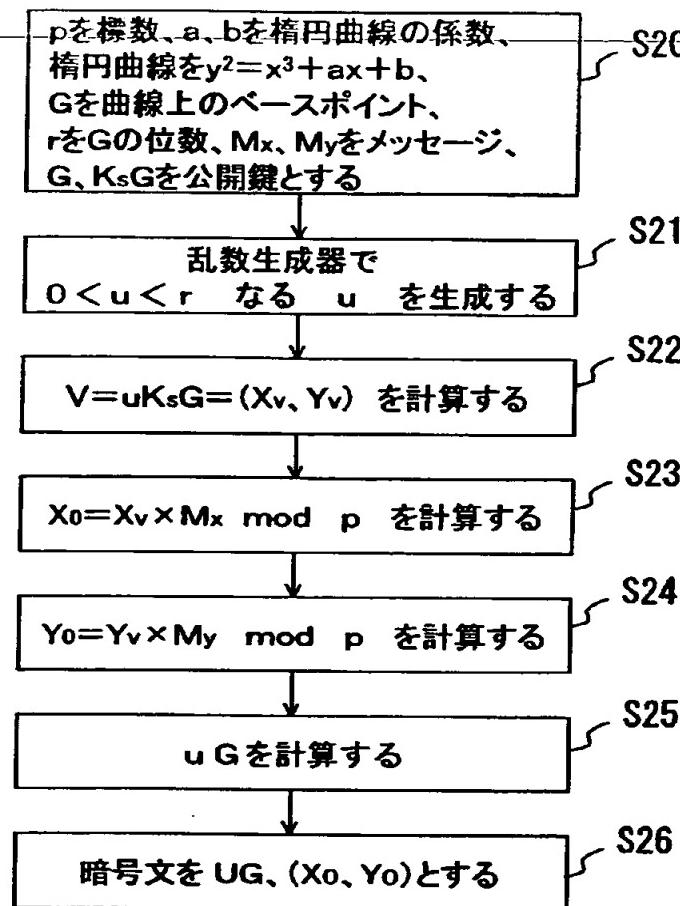


図12 楕円曲線暗号を用いた暗号化 (Menezes-Vanstone) 処理

【図13】

## (復号化)

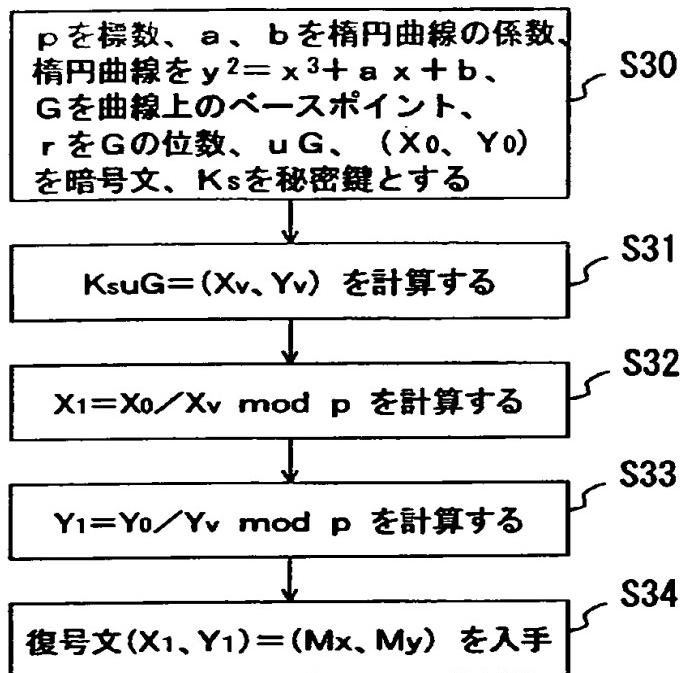


図13 楕円曲線暗号を用いた復号化 (Menezes-Vanstone) 処理

### 【図14】

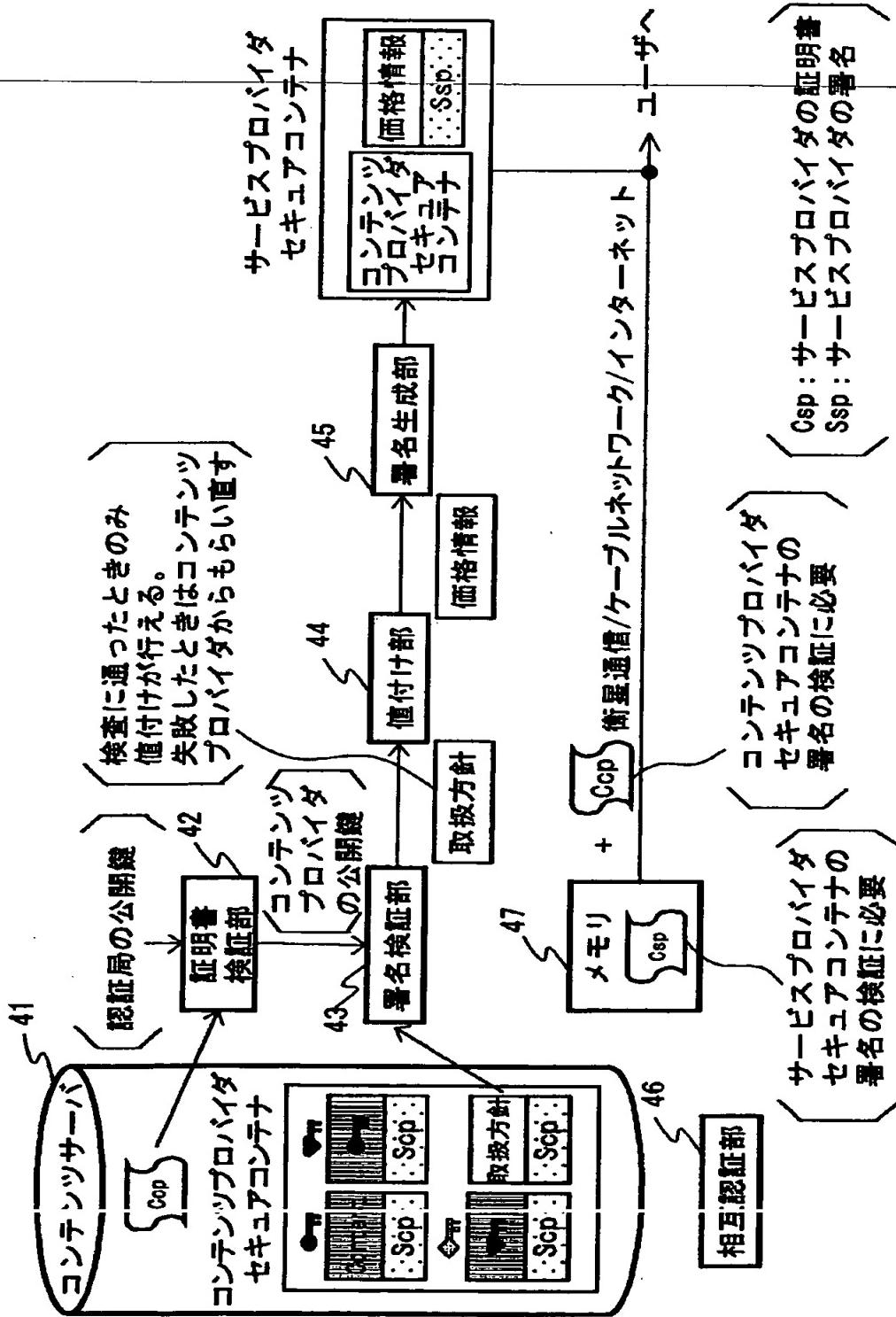


図14 サービスプロバイダの構成

[図15]

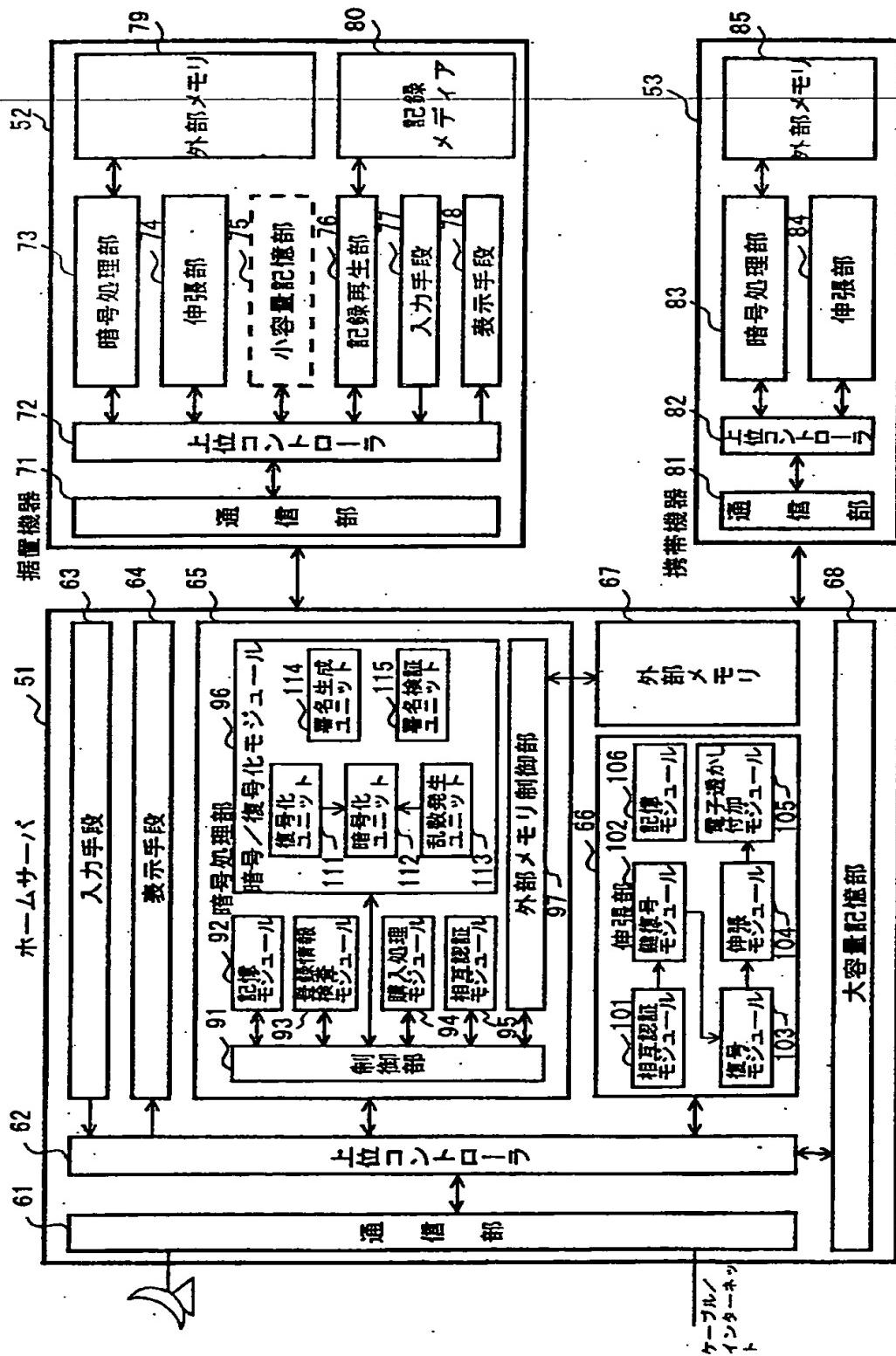
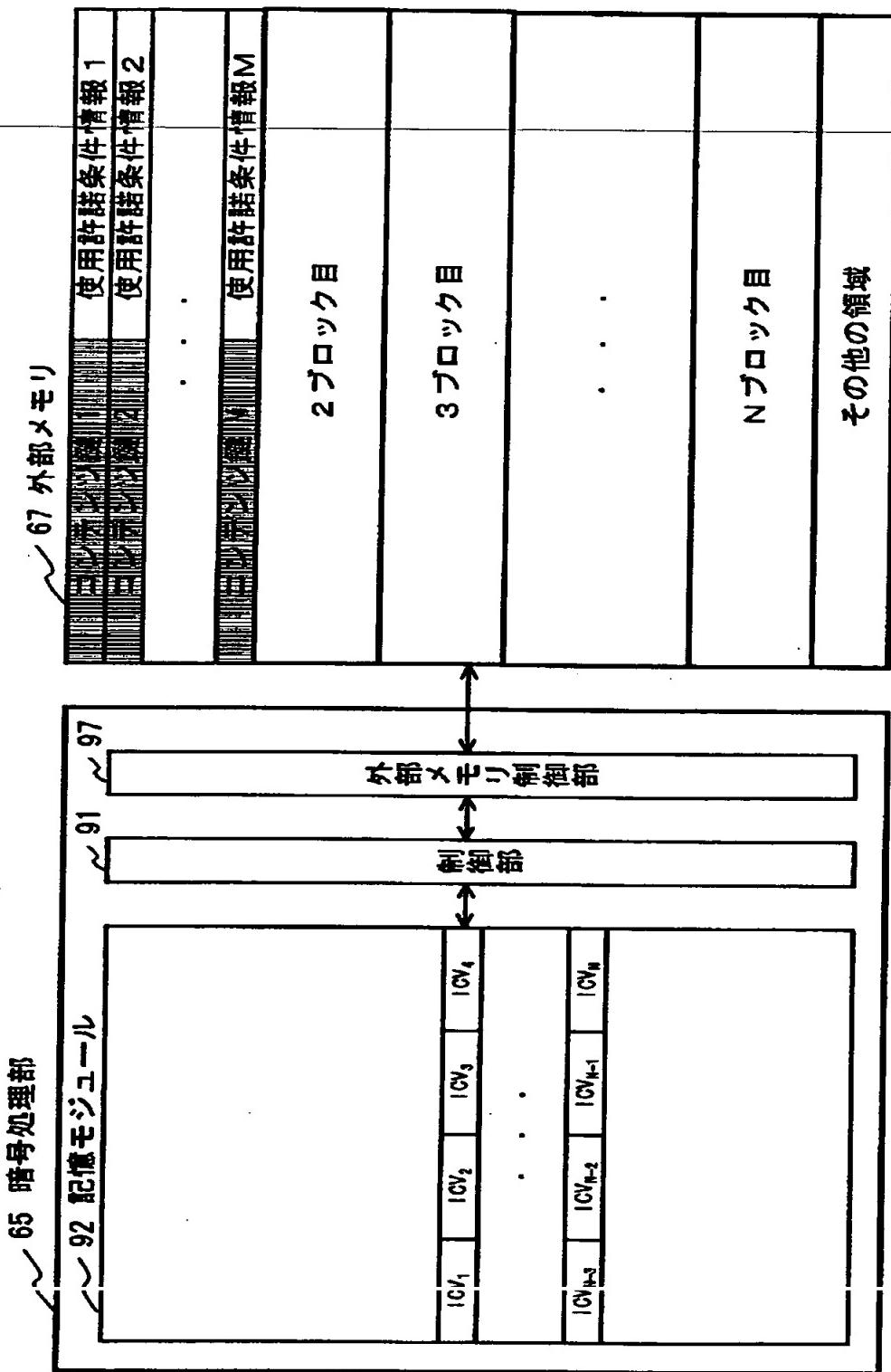


図15 ユーザーホームネットワーク5

【図16】



【図17】

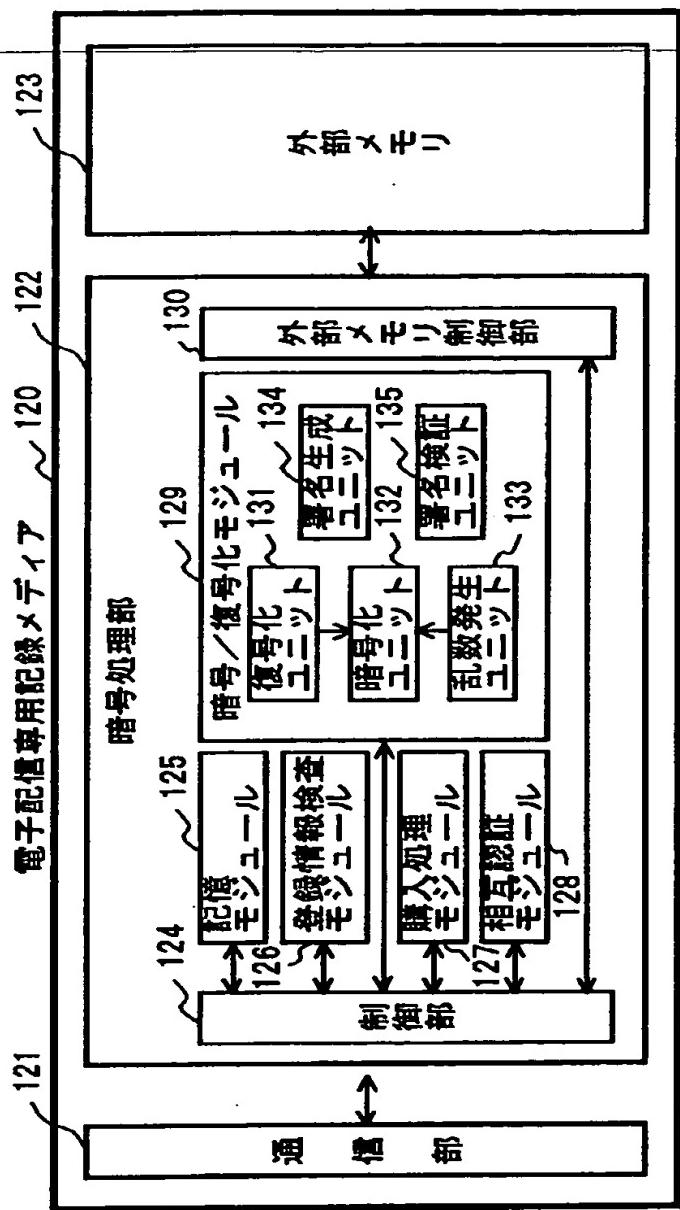
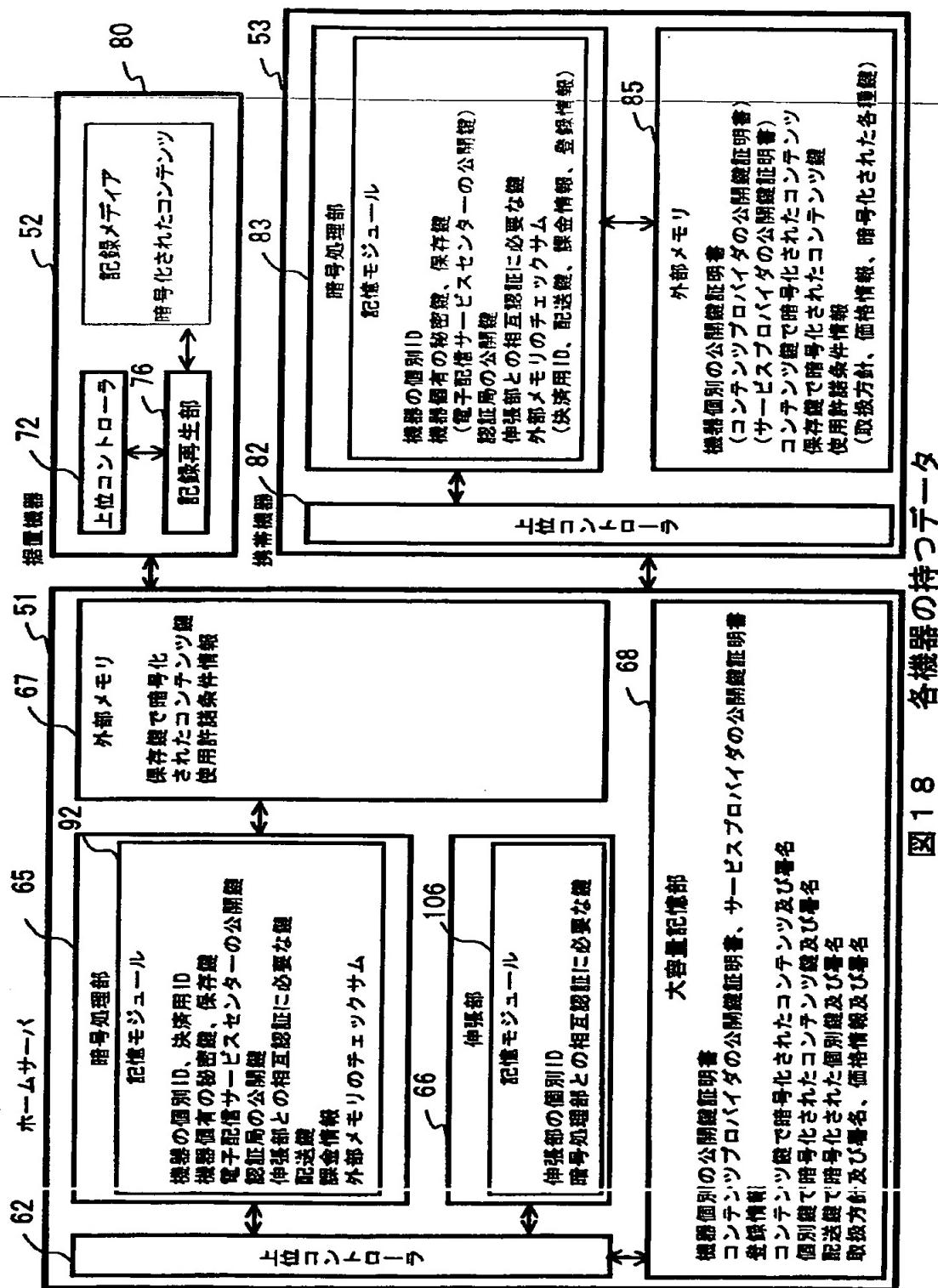


図17 電子配信専用記録メディア

【図18】



【図19】

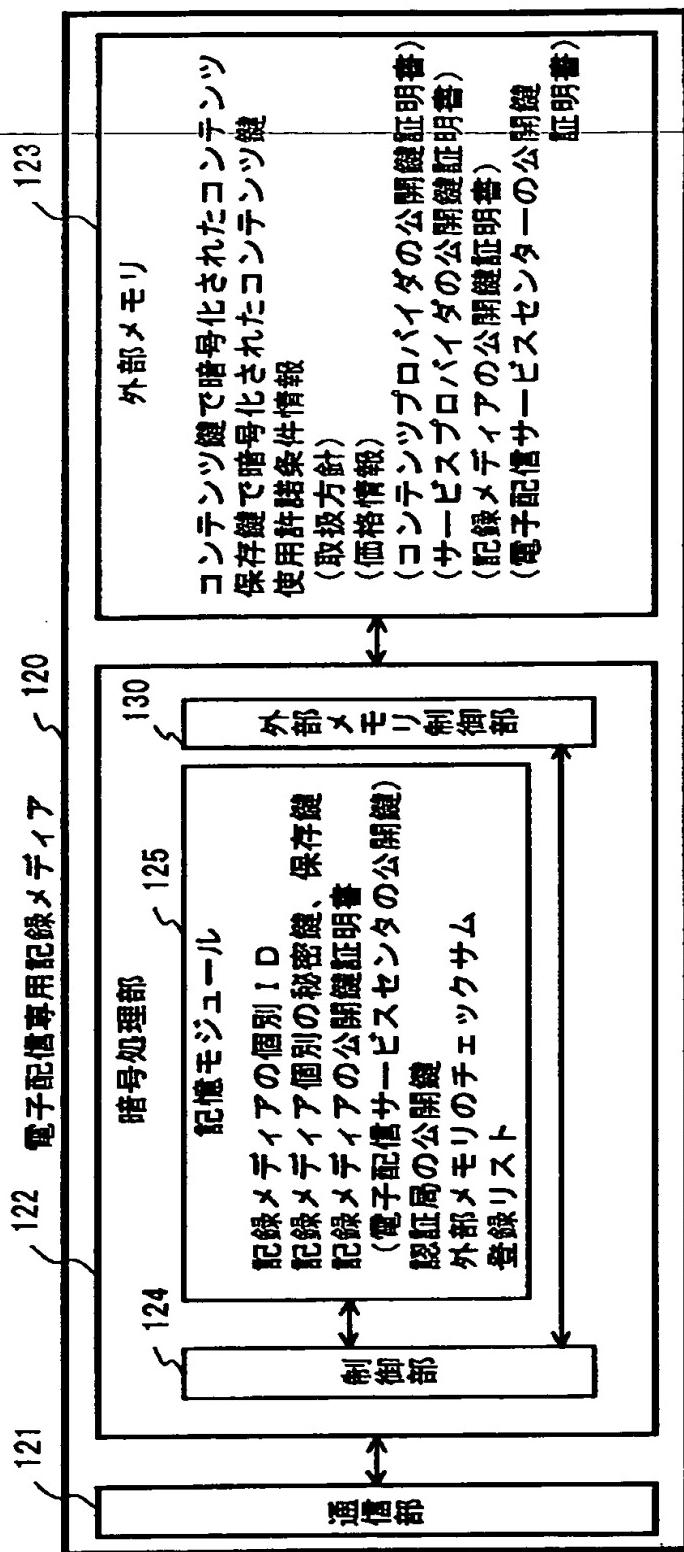
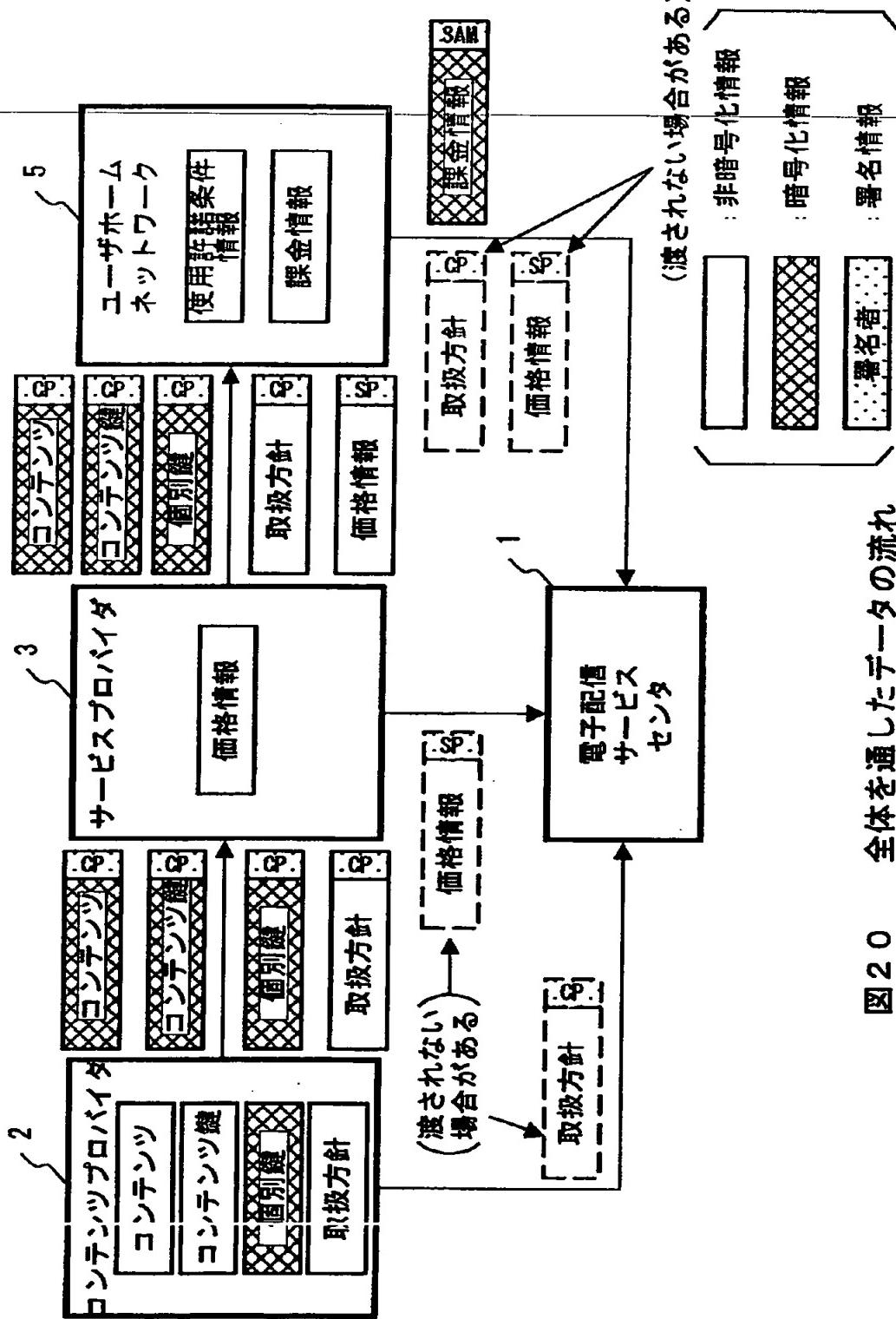


図19 電子配信専用記録メディアの保持するデータ

【図20】



[図21]

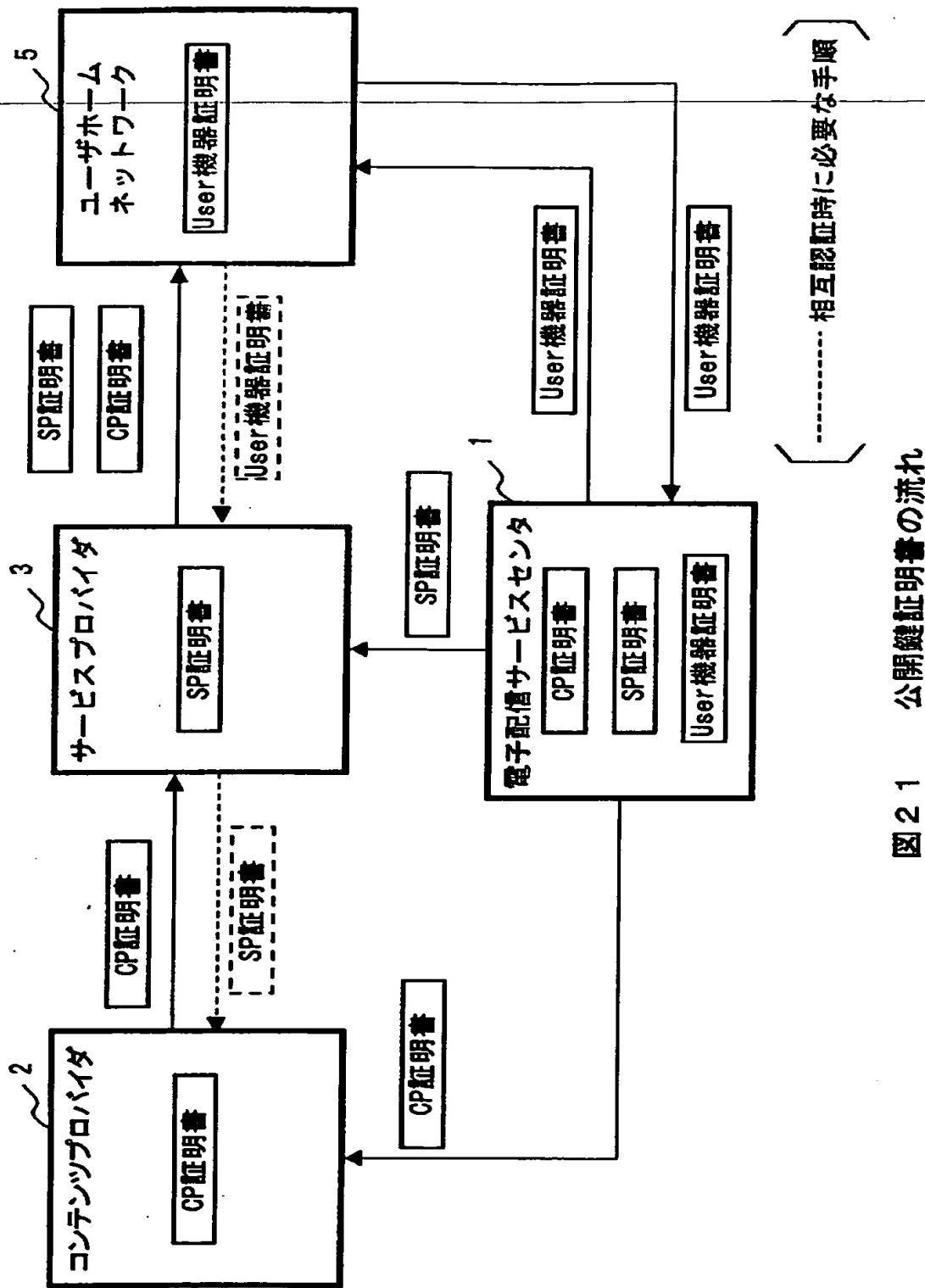


図21 公開鍵証明書の流れ

【図22】

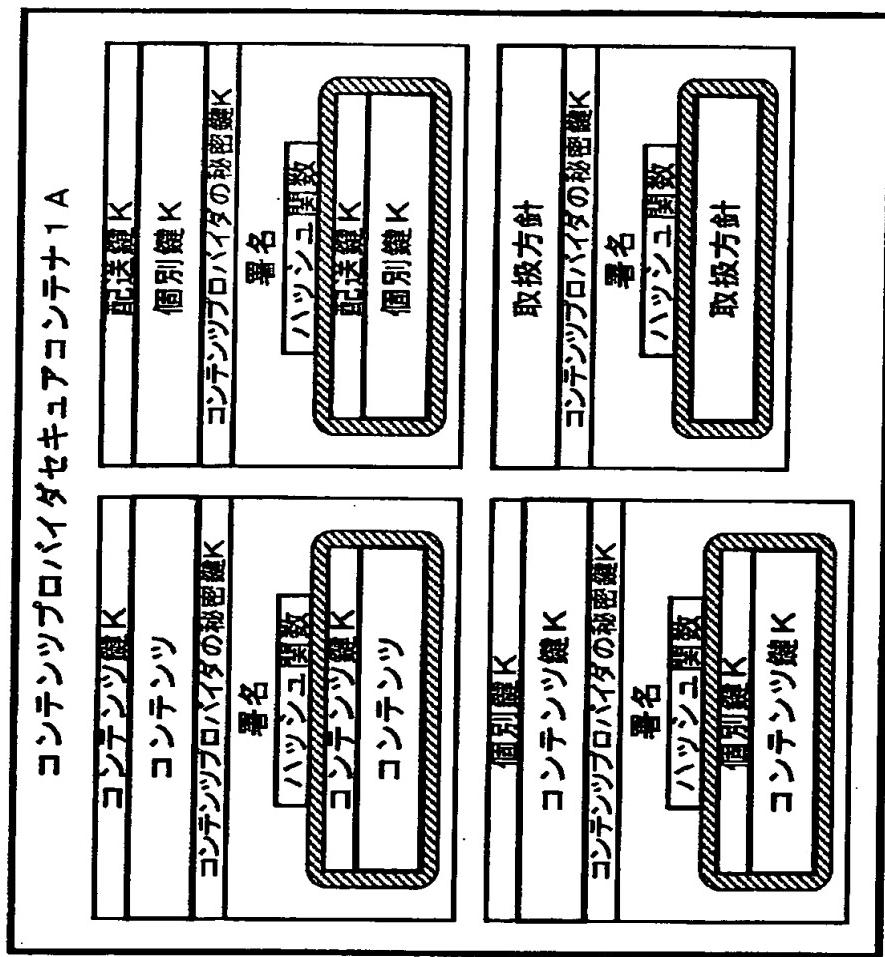


図22 コンテナップロバイダセキュアコンテナ

【図23】

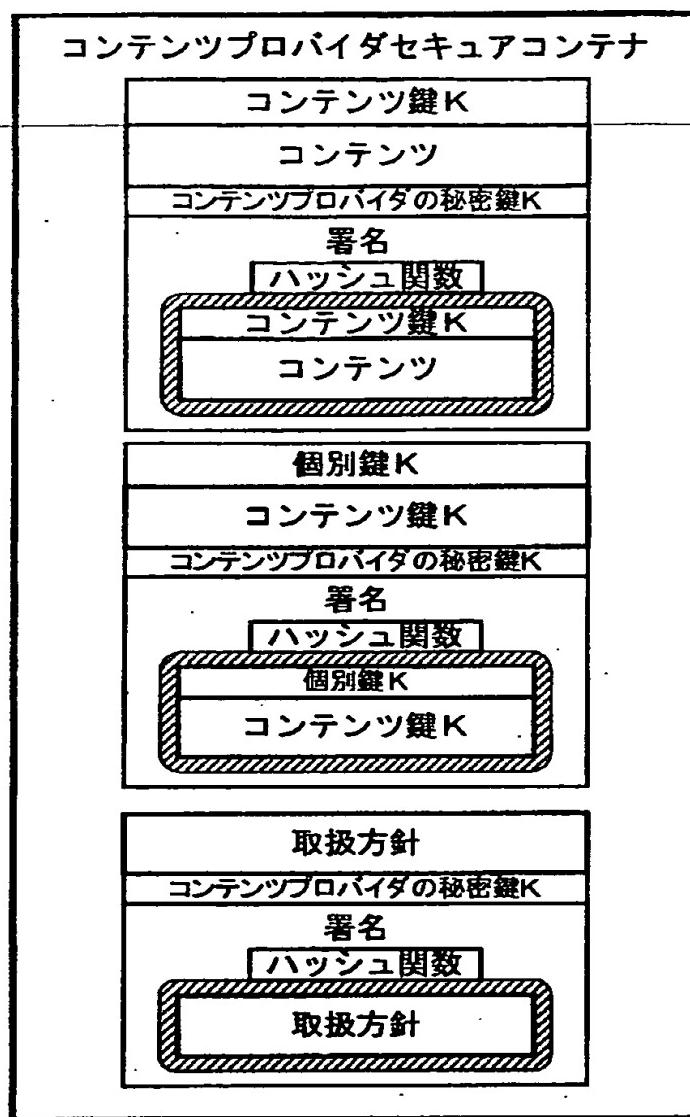


図23 コンテンツプロバイダセキュアコンテナの他の例

【図24】

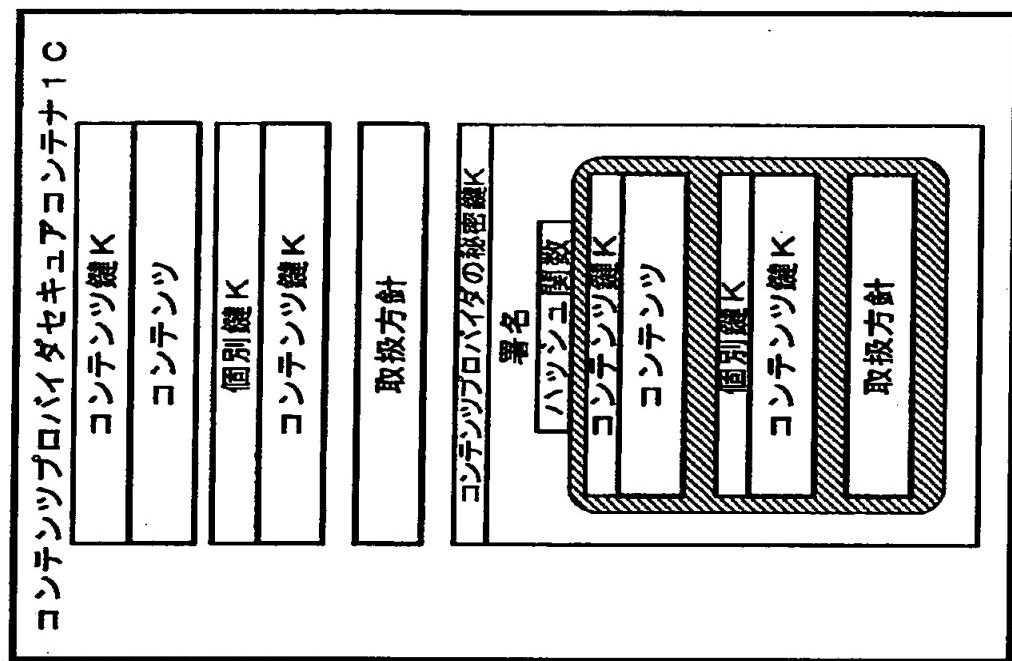


図24 コンテンツプロバイダセキュアコンテナの他の例

【図25】

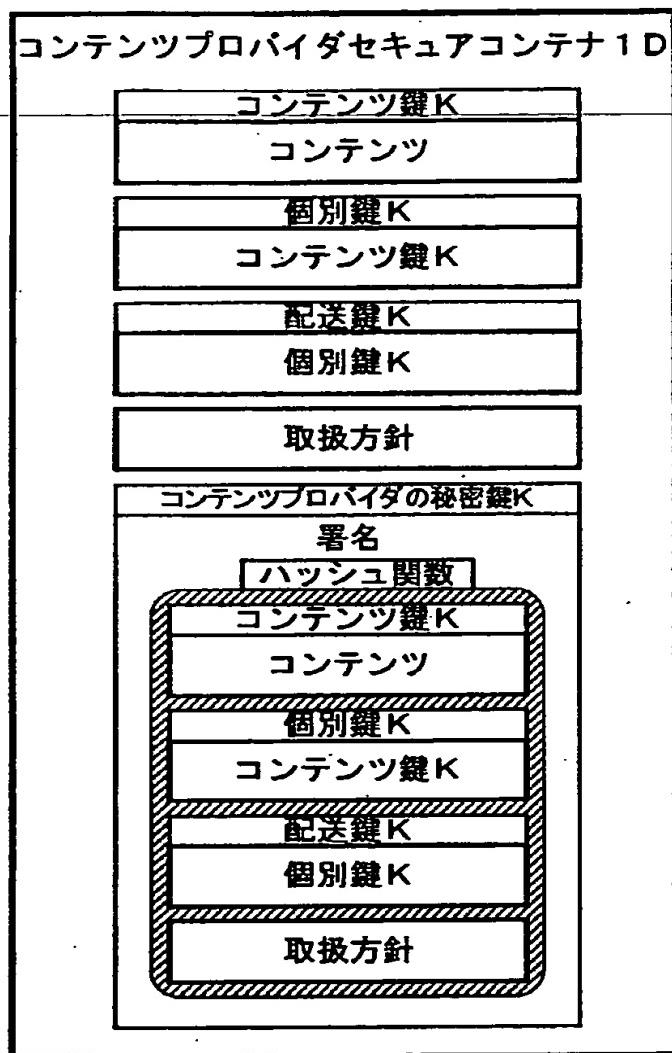


図25 コンテンツプロバイダセキュアコンテナの他の例

【図26】

メッセージ全体

コンテンツプロバイダの証明書2A	
証明書のバージョン番号	認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムビラメータ	認証局の名前
証明書の有効期限	コンテンツプロバイダの名前(ID)
コンテンツプロバイダの公開鍵(Kpcp)	認証局の秘密鍵(KscA)
署名	ハッシュシユート数 メッセージ全体

図26 コンテンツプロバイダの公開鍵証明書

【図27】

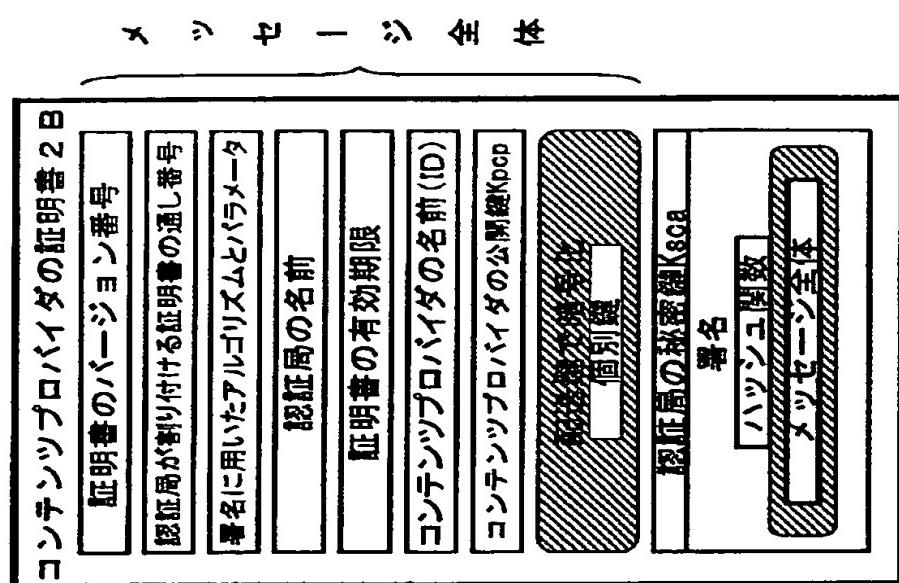


図27 コンテンツプロバイダの公開鍵証明書の他の例

【図28】

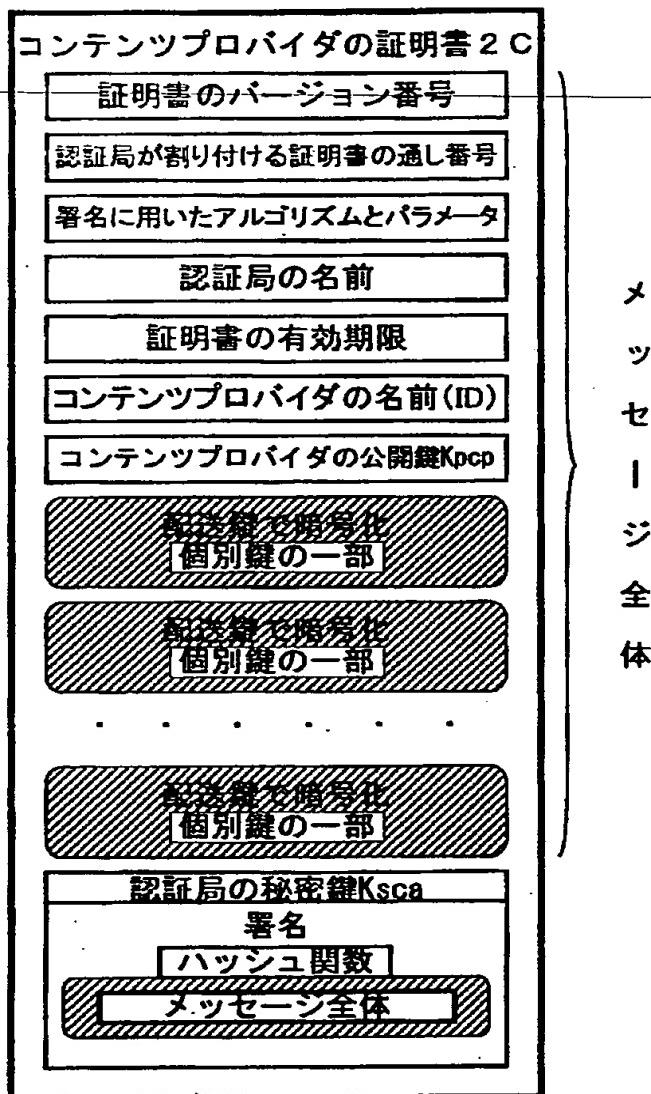


図28 コンテンツプロバイダの公開鍵証明書の他の例

【図29】

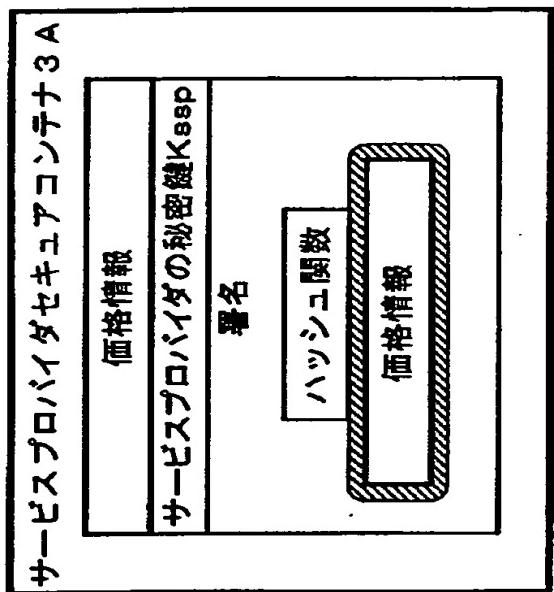


図29 サービスプロバイダセキュアコンテナ

【図30】

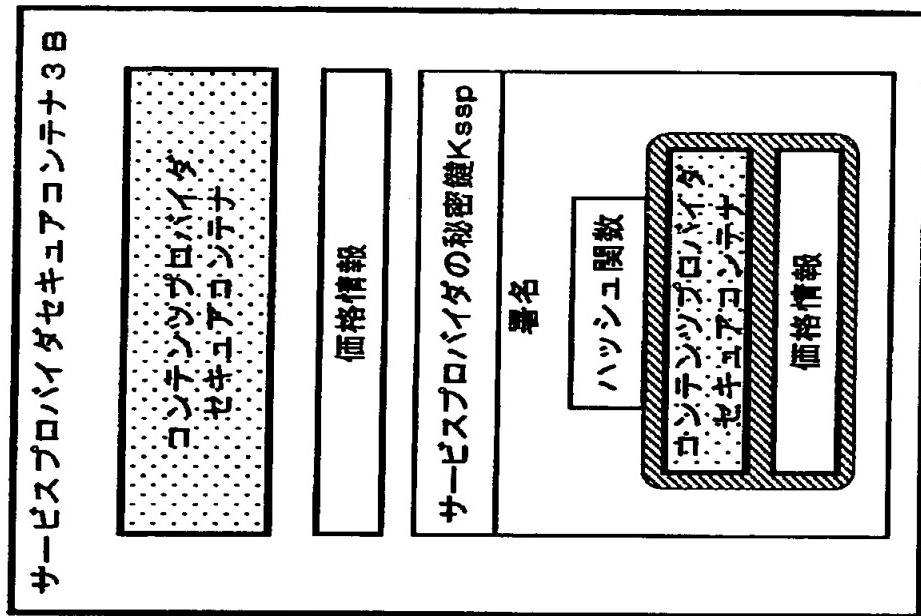


図30 サービスプロバイダセキュアコンテナの他の例

【図31】

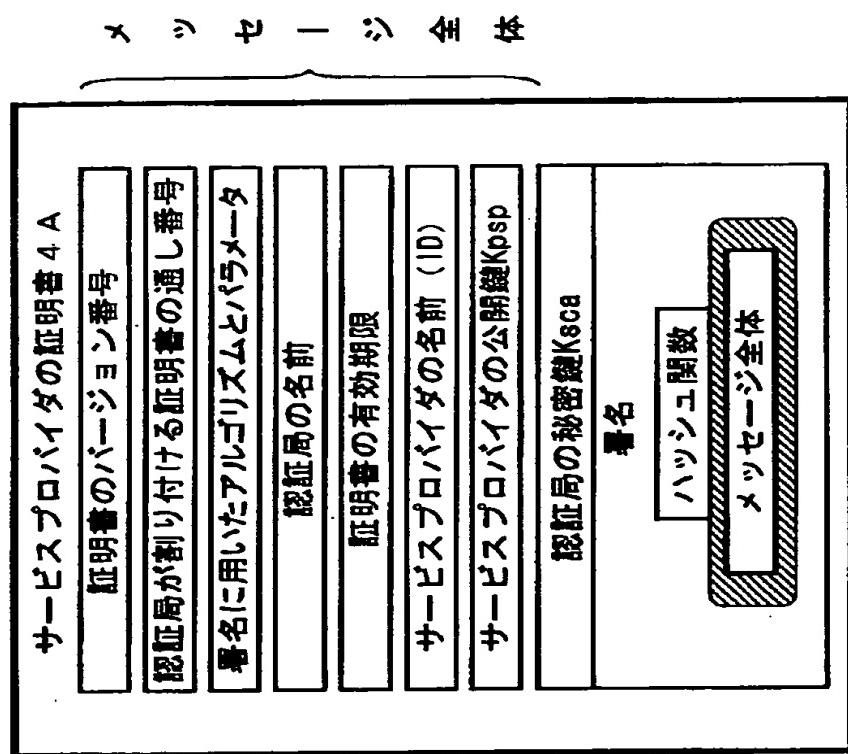


図31 サービスプロバイダの公開鍵証明書

【図32】

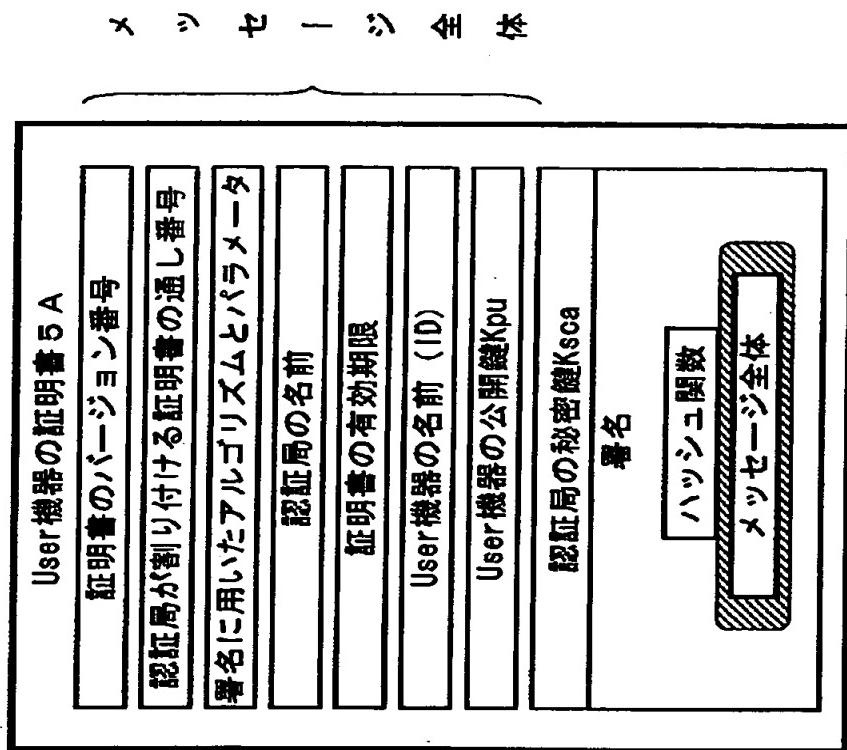


図32 User機器の公開鍵証明書

【図33】

データの種別	
取扱方針の種類（シングル）	
取扱方針の有効期限	
コンテンツのID	
コンテンツプロバイダのID	
取扱方針のID	
取扱方針のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのID	
世代管理情報	
ルールの数	
ルールのアドレス情報	
ル ル 1	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
ル ル N	送信情報
	：
	：
	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
コンテンツプロバイダの利益額	
コンテンツプロバイダの利益率	
データサイズ	
送信情報	
(署名の検証の有無)	
公開鍵証明書	
署名	

図33 シングルコンテンツの取扱方針

【図34】

データの種別	
	取扱方針の種類（アルバム）
	取扱方針の有効期限
	アルバムのID
	取扱方針のバージョン
	コンテンツプロバイダのID
	取扱方針のID
	地域コード
	使用可能機器条件
	使用可能User条件
	サービスプロバイダのID
	シングルコンテンツの取扱方針の数
	シングルコンテンツの取扱方針のアドレス情報
シングル	取扱方針1
	⋮
ルール	取扱方針N
	世代管理情報
ルール	ルールの数
	ルールのアドレス情報
ルール1	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
ルールN	送信情報
	⋮
	⋮
	⋮
	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
ルールN	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
	送信情報
	(署名の検出の有無)
	公開鍵証明書
署名	

図34 アルバムコンテンツの取扱方針

【図35】

データの種別	
取扱方針の種類（シングル）	
取扱方針の有効期限	
コンテンツのID	
コンテンツプロバイダのID	
取扱方針のID	
取扱方針のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのID	
世代管理情報	
ルールの数	
ルールのアドレス情報	
ル ー ル 1	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	データサイズ
	送信情報
ル ー ル N	•
	•
	•
	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
最低販売価格	
データサイズ	
送信情報	
(署名の検出の有無)	
公開鍵証明書	
署名	

図35 シングルコンテンツの取扱方針のその他の例

【図36】

データの種別	
取扱方針の種類（アルバム）	
取扱方針の有効期限	
アルバムのID	
取扱方針のバージョン	
コンテンツプロバイダのID	
取扱方針のID	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのID	
シングルコンテンツの取扱方針の数	
シングルコンテンツの取扱方針のアドレス情報	
シングル	取扱方針1
	⋮
シングル	取扱方針N
	世代管理情報
ルール	ルールの数
	ルールのアドレス情報
ルール1	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	データサイズ
	送信情報
ルールN	⋮
	⋮
	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
(署名の検出の有無)	
公開鍵証明書	
署名	

図36 アルバムコンテンツの取扱方針のその他の例

【図37】

データの種別	
価格情報の種類（シングル）	
価格情報の有効期限	
コンテンツのID	
サービスプロバイダのID	
価格情報のID	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのID	
取扱方針のID	
ルールの数	
ルールのアドレス情報	
ル ル ル ル ル ル	ルール番号 (Rule#)
	サービスプロバイダの利益額
	サービスプロバイダの利益率
	価格
	データサイズ
	送信情報
ル ル ル ル ル ル ル	ルール番号 (Rule#)
	サービスプロバイダの利益額
	サービスプロバイダの利益率
	価格
	データサイズ
	送信情報
	(署名の検出の有無)
公開鍵証明書	
署名	

図37 シングルコンテンツの価格情報

【図38】

データの種別	
価格情報の種類（アルバム）	
価格情報の有効期限	
アルバムのID	
サービスプロバイダのID	
価格情報のID	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのID	
取扱方針のID	
シングルコンテンツの価格情報の数	
シングルコンテンツの価格情報のアドレス情報	
シングル	価格情報1
	・ ・
ルール	価格情報N
	ルールの数
ルールのアドレス情報	
ルール1	ルール番号 (Rule#)
	サービスプロバイダの利益額
ルール2	サービスプロバイダの利益率
	価格
ルール3	データサイズ
	送信情報
ルール4	・ ・
	・ ・
ルール5	ルール番号 (Rule#)
	サービスプロバイダの利益額
ルール6	サービスプロバイダの利益率
	価格
ルール7	データサイズ
	送信情報
(署名の検出の有無)	
公開鍵証明書	
署名	

図38 アルバムコンテンツの価格情報

【図39】

データの種別	
価格情報の種類（シングル）	
価格情報の有効期限	
コンテンツのID	
サービスプロバイダのID	
価格情報のID	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのID	
取扱方針のID	
ルールの数	
ルールのアドレス情報	
ル	ルール番号 (Rule#)
ー	価格
ル	データサイズ
1	送信情報
⋮	⋮
ル	ルール番号 (Rule#)
ー	価格
ル	データサイズ
N	送信情報
(署名の検出の有無)	
公開鍵証明書	
署名	

図39 シングルコンテンツの価格情報の他の例

【図40】

データの種別	
価格情報の種類（アルバム）	
価格情報の有効期限	
アルバムのID	
サービスプロバイダのID	
価格情報のID	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのID	
取扱方針のID	
シングルコンテンツの価格情報の数	
シングルコンテンツの価格情報のアドレス情報	
シングル	価格情報1
	• • •
シングル	価格情報N
	ルールの数
ルールのアドレス情報	
ルール1	ルール番号 (Rule#)
	価格
	データサイズ
	送信情報
• • •	• • •
ルールN	ルール番号 (Rule#)
	価格
	データサイズ
	送信情報 (署名の検出の有無)
公開鍵証明書	
署名	

図40 アルバムコンテンツの価格情報の他の例

【図41】

データの種別
使用許諾条件情報の種類
使用許諾条件情報の有効期限
コンテンツのID
アルバムのID
暗号処理部のID
ユーザのID
コンテンツプロバイダのID
取扱方針のID
取扱方針のバージョン
サービスプロバイダのID
価格情報のID
価格情報のバージョン
使用許諾条件情報のID
再生権（利用権）のルール番号
利用権内容番号
再生残り回数
再生権の有効期限
複製権（利用権）のルール番号
利用権内容番号
複製残り回数
世代管理情報
再生権を保有する暗号処理部のID

図41 使用許諾条件情報

【図42】

データの種別
暗号処理部のID
ユーザのID
コンテンツのID
コンテンツプロバイダのID
取扱方針のID
取扱方針のバージョン
サービスプロバイダのID
価格情報のID
価格情報のバージョン
使用許諾条件のID
ルール番号 (Rule#)
コンテンツプロバイダの利益額／利益率
サービスプロバイダの利益額／利益率
世代管理情報
コンテンツプロバイダの設定した送信情報のデータサイズ
コンテンツプロバイダの設定した送信情報
サービスプロバイダの設定した送信情報のデータサイズ
サービスプロバイダの設定した送信情報
供給元のID

図42 課金情報

【図43】

データの種別
暗号処理部のID
ユーザのID
コントローラのID
コンテンツプロバイダのID
取扱方針のID
取扱方針のバージョン
サービスプロバイダのID
価格情報のID
価格情報のバージョン
使用許諾条件のID
ルール番号 (Rule#)
世代管理情報
コンテンツプロバイダの設定した送信情報のデータサイズ
コンテンツプロバイダの設定した送信情報
サービスプロバイダの設定した送信情報のデータサイズ
サービスプロバイダの設定した送信情報
供給元のID

図43 課金情報の他の例

【図44】

利用権内容番号	利用権内容			
	権利	期間制限	回数制限	複製制限
(1)		なし	なし	—
(2)	再生権	あり	なし	—
(3)		あり	なし	—
(4)		なし	なし	—
(5)		なし	あり	—
(6)	複製権	なし	なし	なし
(7)		なし	あり	なし
(8)		なし	なし	—
(9) ~ (15)		なし	あり	S CMS 予備
(16)	権利内容変更権	—	—	—
(17)	再購入権	—	—	—
(18)	追加購入権	—	—	—
(19)	管理移動権	—	—	—

図44 利用権内容の一覧

【図45】

(A)	再生権の有効期限
(B)	再生権の有効期限
(C)	再生権の有効期限 日数及び時間
(D)	再生権の有効期限 再生回数
(E)	複製権の有効期限
(F)	複製権の有効期限 複製回数
(G)	複製権の有効期限
(H)	複製権の有効期限 複製回数
(I)	権利内容変更権の有効期限 旧ルール番号 新ルール番号
(J)	再購入権の有効期限 旧ルール番号 新ルール番号 最大再配信世代情報
(K)	追加購入権の有効期限 最小保有コンテンツ番号 最大保有コンテンツ番号
(L)	管理移動権の有効期限
(M)	コンテンツ購入権の有効期限 旧コンテンツのID 旧ルール番号 新ルール番号

図45 利用権

【図46】

データの種別
コンテンツの種類(シングル)
コンテンツの有効期限
コンテンツのカテゴリー
コンテンツのID
コンテンツプロバイダのID
コンテンツの暗号方式
暗号化したコンテンツのデータ長
暗号化したコンテンツ
公開鍵証明書
署名

図46 シングルコンテンツ

【図47】

データの種別	
コンテンツの種類（アルバム）	
コンテンツの有効期限	
アルバムのID	
コンテンツプロバイダのID	
シングルコンテンツの数	
シングルコンテンツのアドレス情報	
シングル	コンテンツ1
	⋮
	コンテンツN
公開鍵証明書	
署名	

図47 アルバムコンテンツ

【図48】

データの種別
鍵データの種類（シングル）
鍵の有効期限
コンテンツのID
コンテンツプロバイダのID
鍵のバージョン
コンテンツ鍵の暗号方式
暗号化したコンテンツ鍵
個別鍵の暗号方式
暗号化した個別鍵
公開鍵証明書
署名

図48 シングルコンテンツ用の鍵データ

【図49】

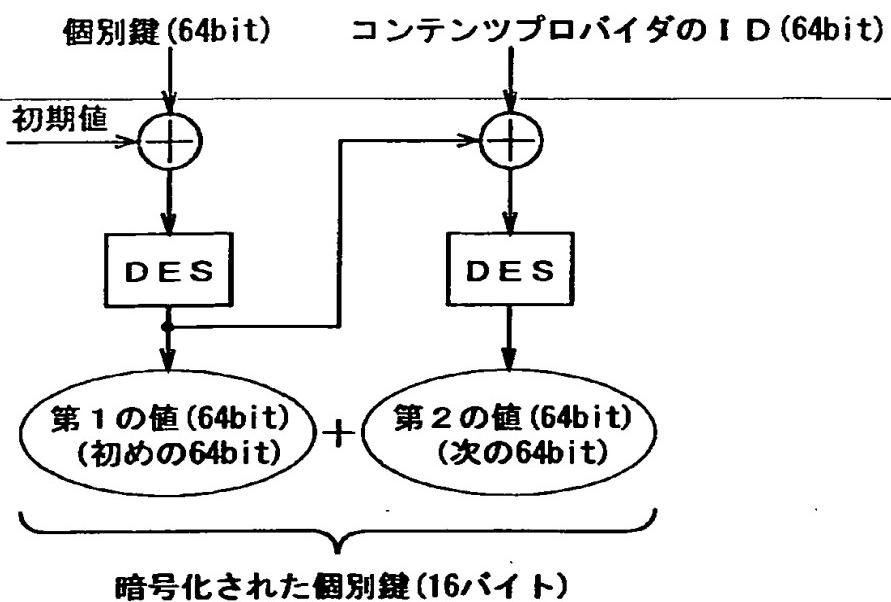


図49 個別鍵の暗号化処理 (Triple-DES-CBC)

【図50】

データの種別	
	鍵データの種類（アルバム）
	鍵の有効期限
	アルバムのID
	コンテンツプロバイダID
	鍵のバージョン
	シングルコンテンツ用の鍵データの数
	シングルコンテンツ用の鍵データのアドレス情報
シ ン グ ル	鍵データ1 ⋮ ⋮ 鍵データN
	公開鍵証明書
	署名

図50 アルバムコンテンツ用の鍵データ

【図 5.1】

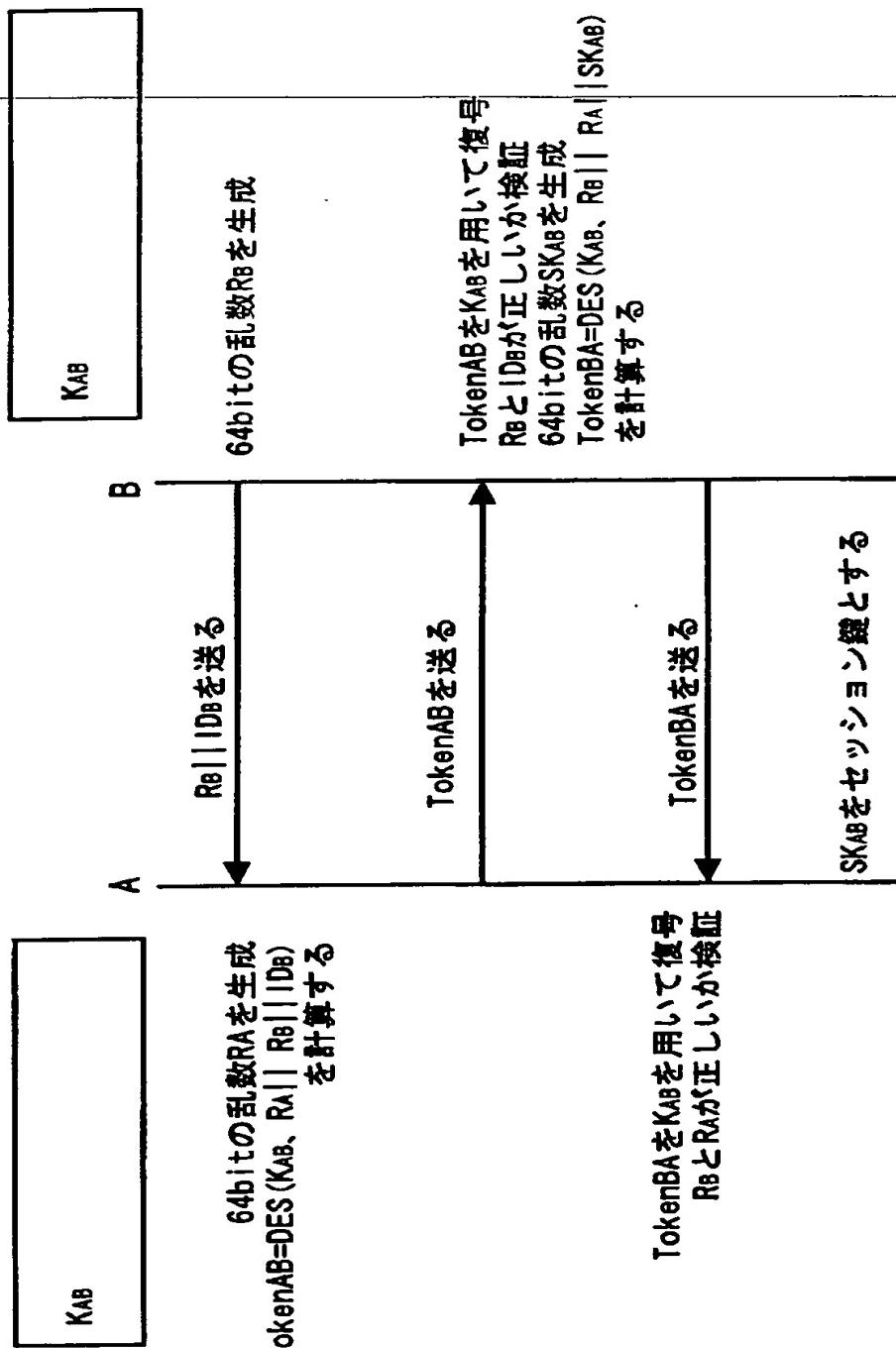


図 5.1 対称鍵暗号技術を用いた相互認証 (ISO/IEC 9798-2)

【図52】

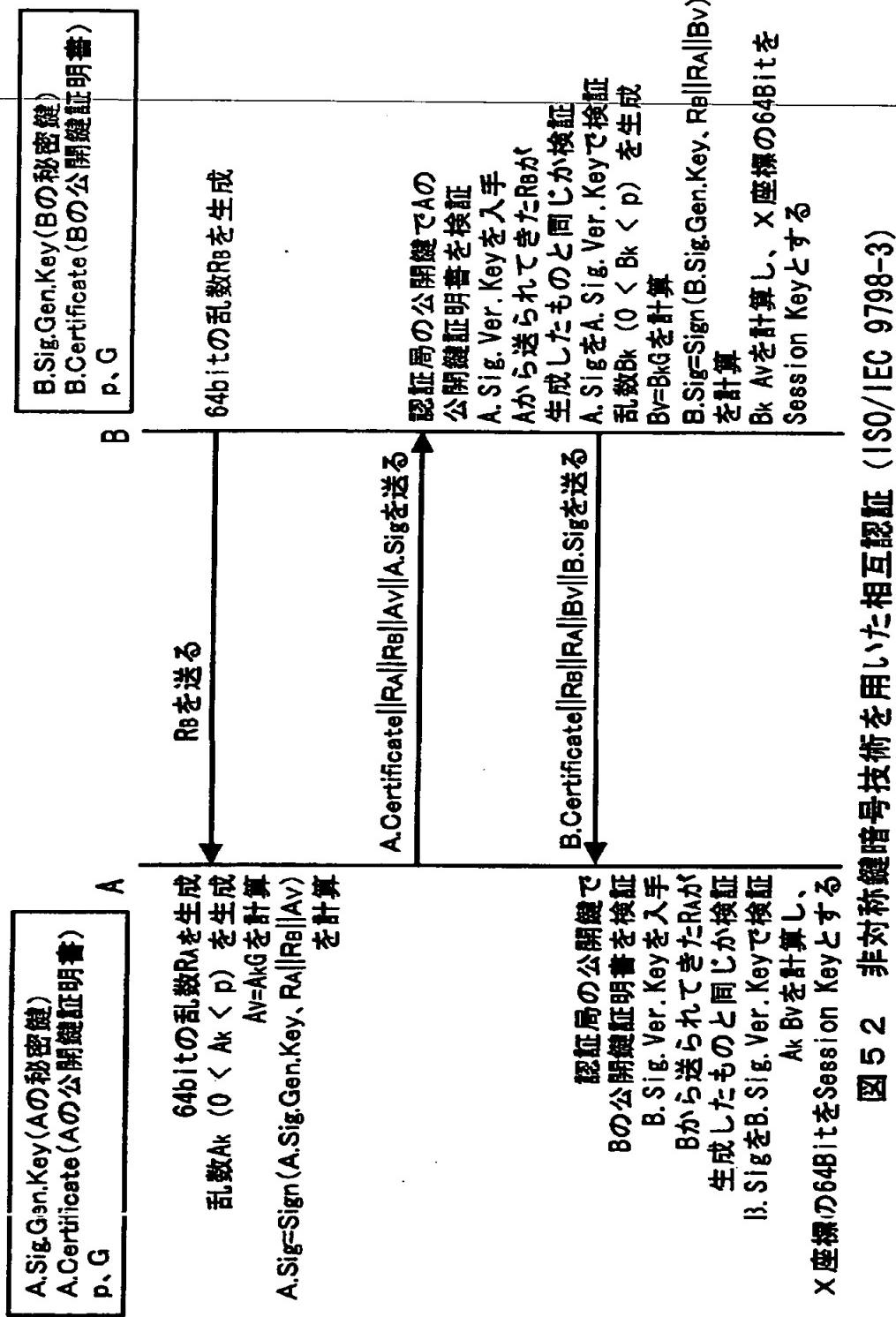


図52 非対称鍵暗号技術を用いた相互認証 (ISO/IEC 9798-3)

[図 5 3]

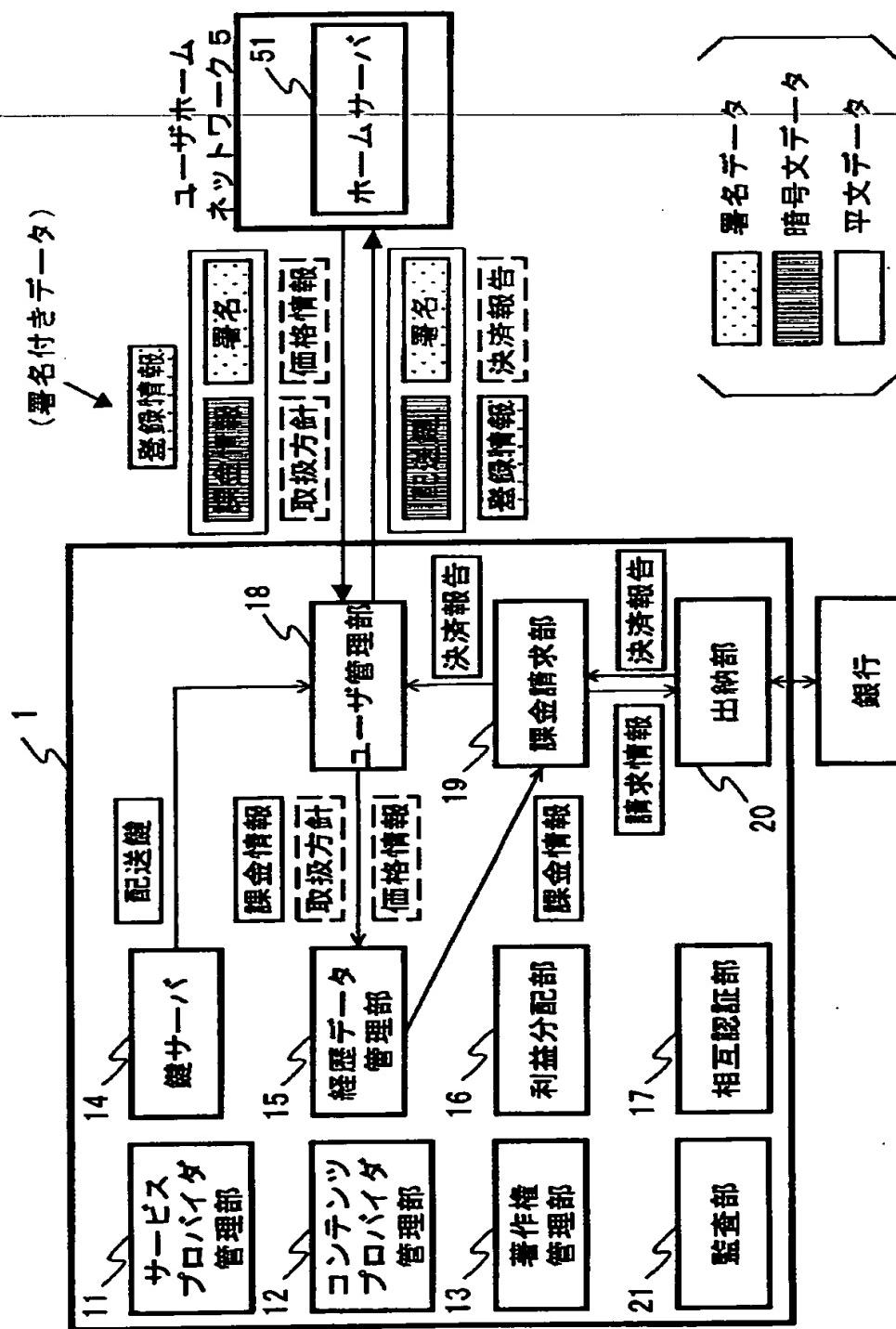


図 5-3 課金情報の送信動作

【図54】

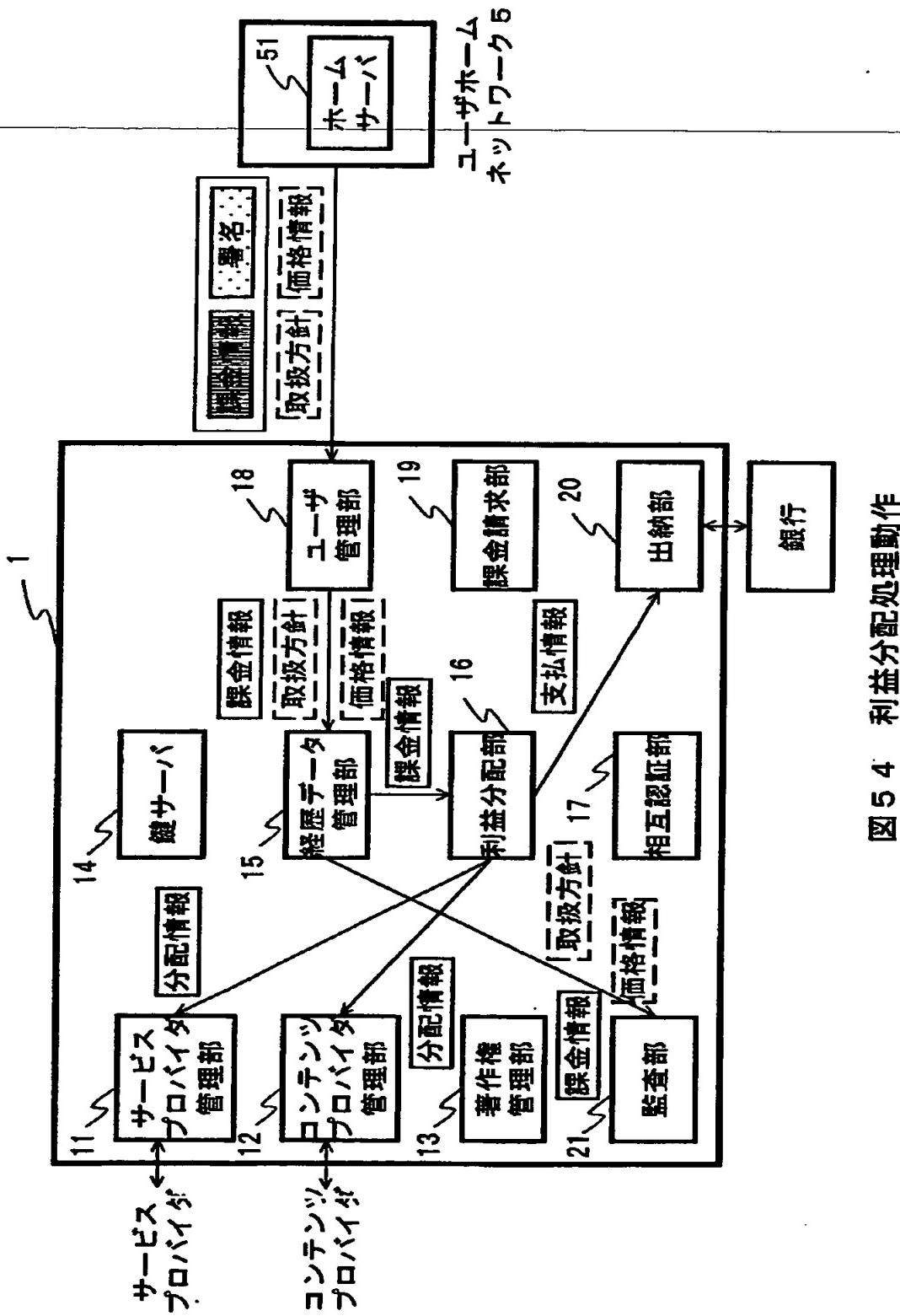


図54 利益分配処理動作

【図55】

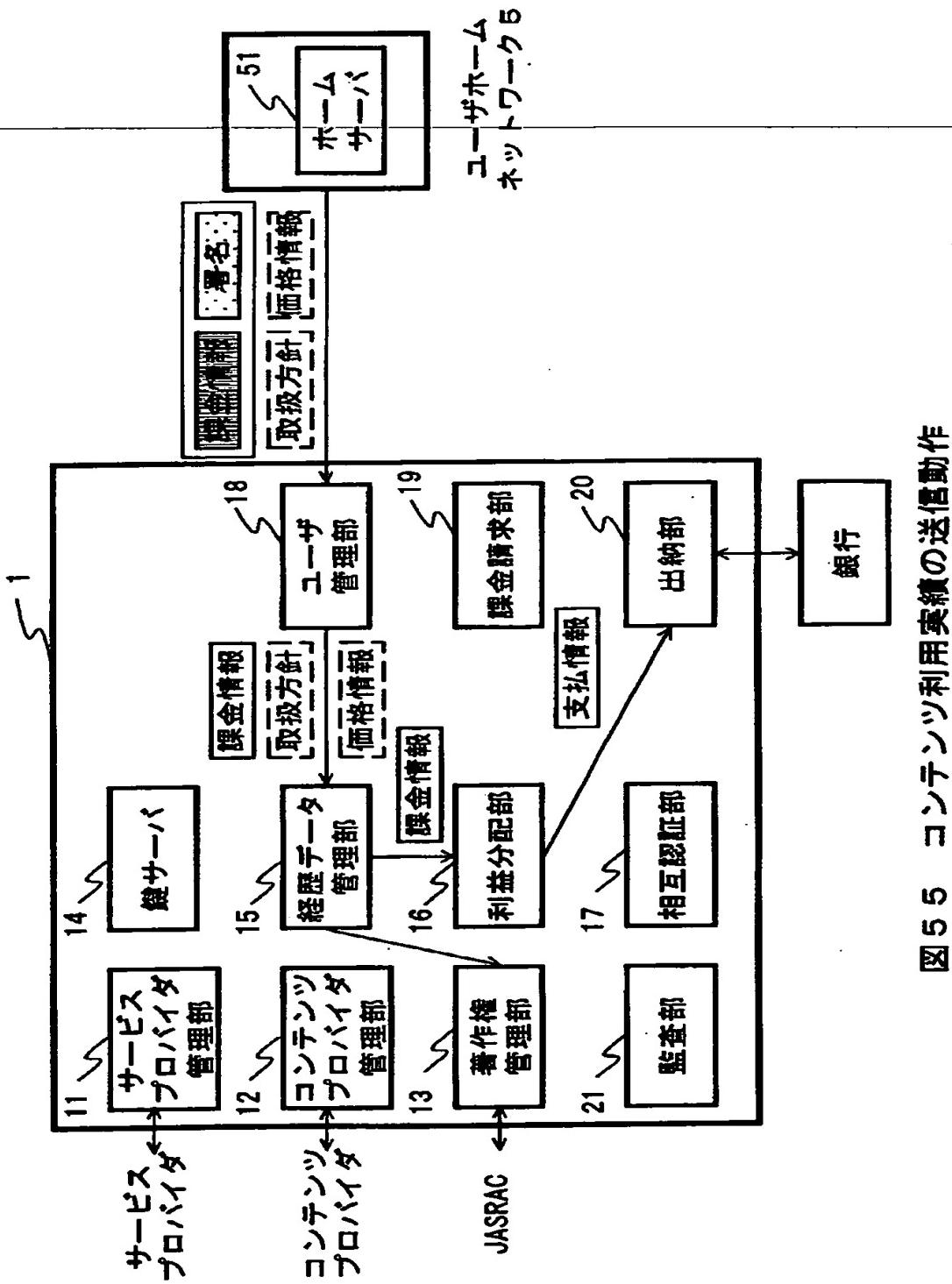


図55 コンテンツ利用実績の送信動作

【図56】

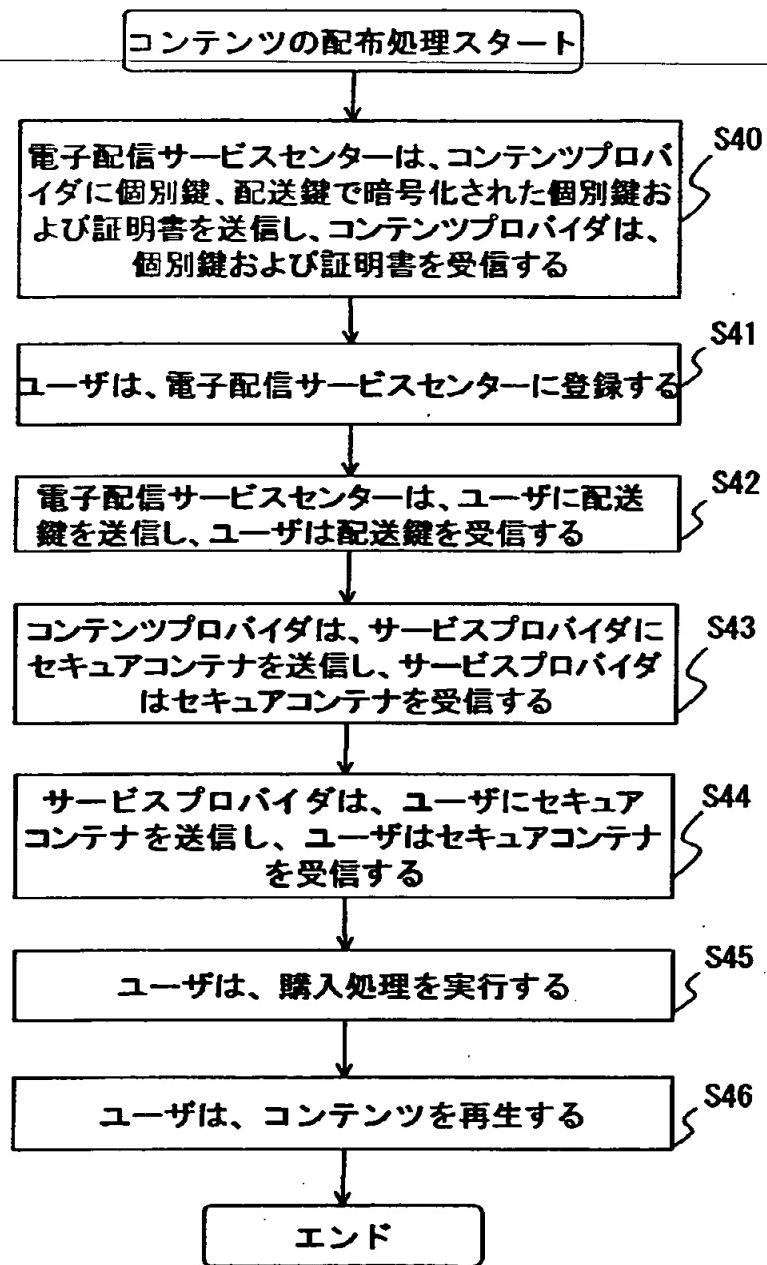


図56 EDMシステムのコンテンツ配布、再生処理手順

【図57】

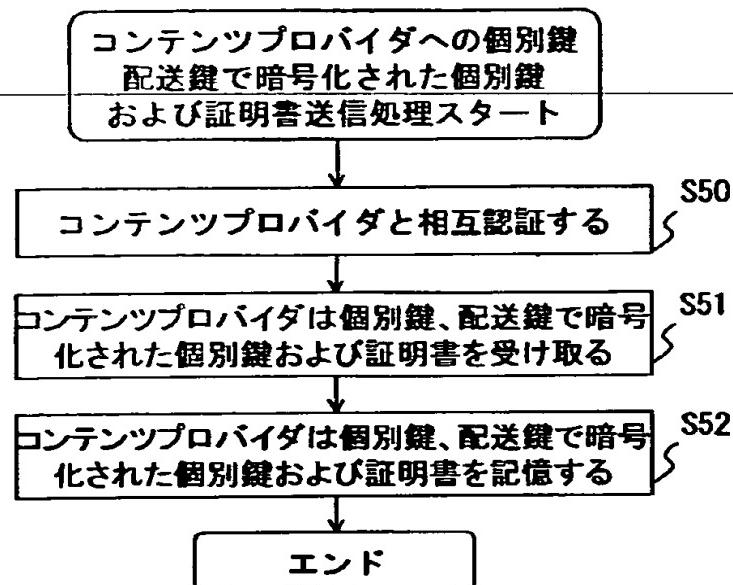


図57 コンテンツプロバイダへの送信処理手順

【図58】

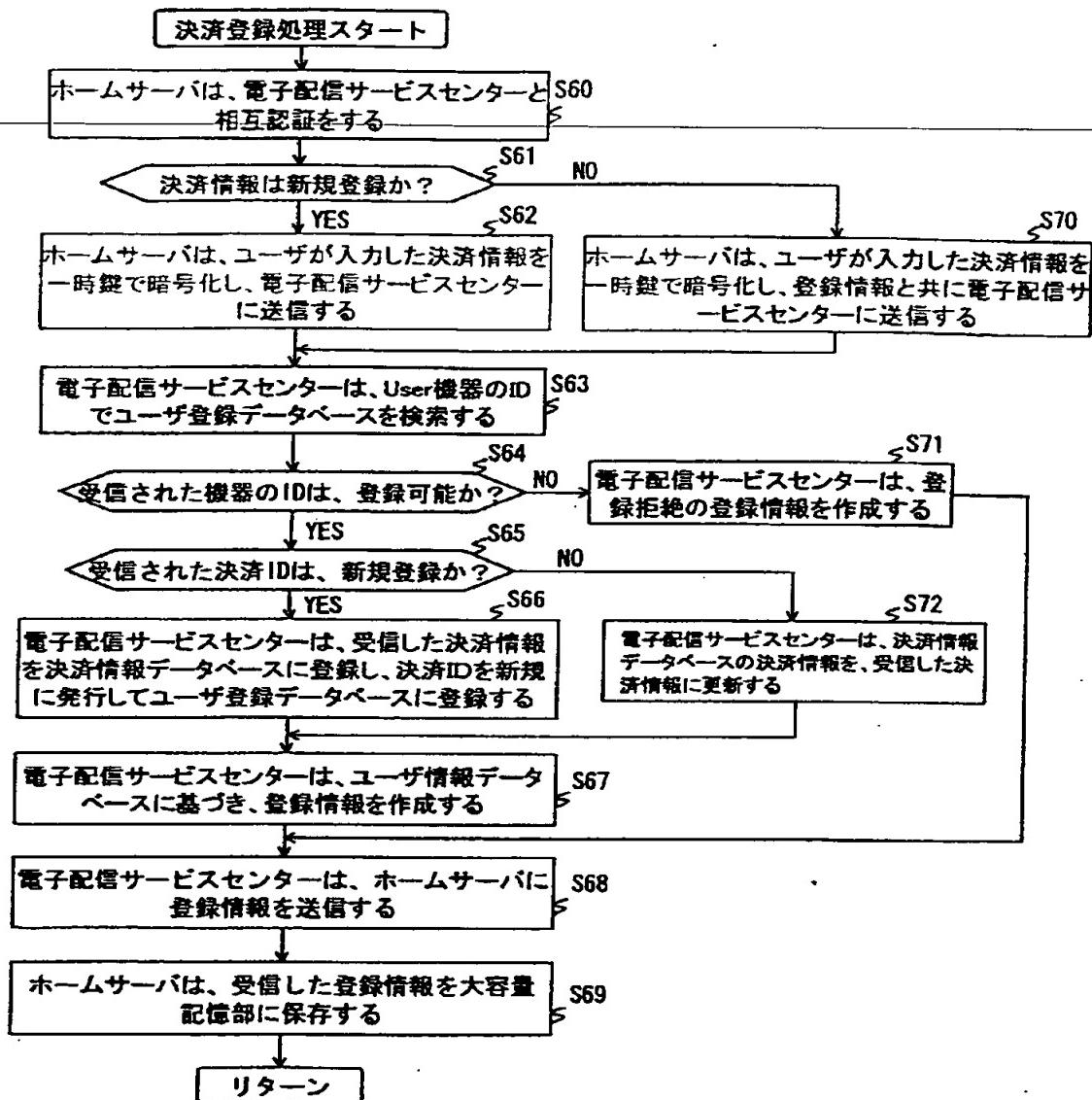


図58 決済情報の登録処理手順

【図59】

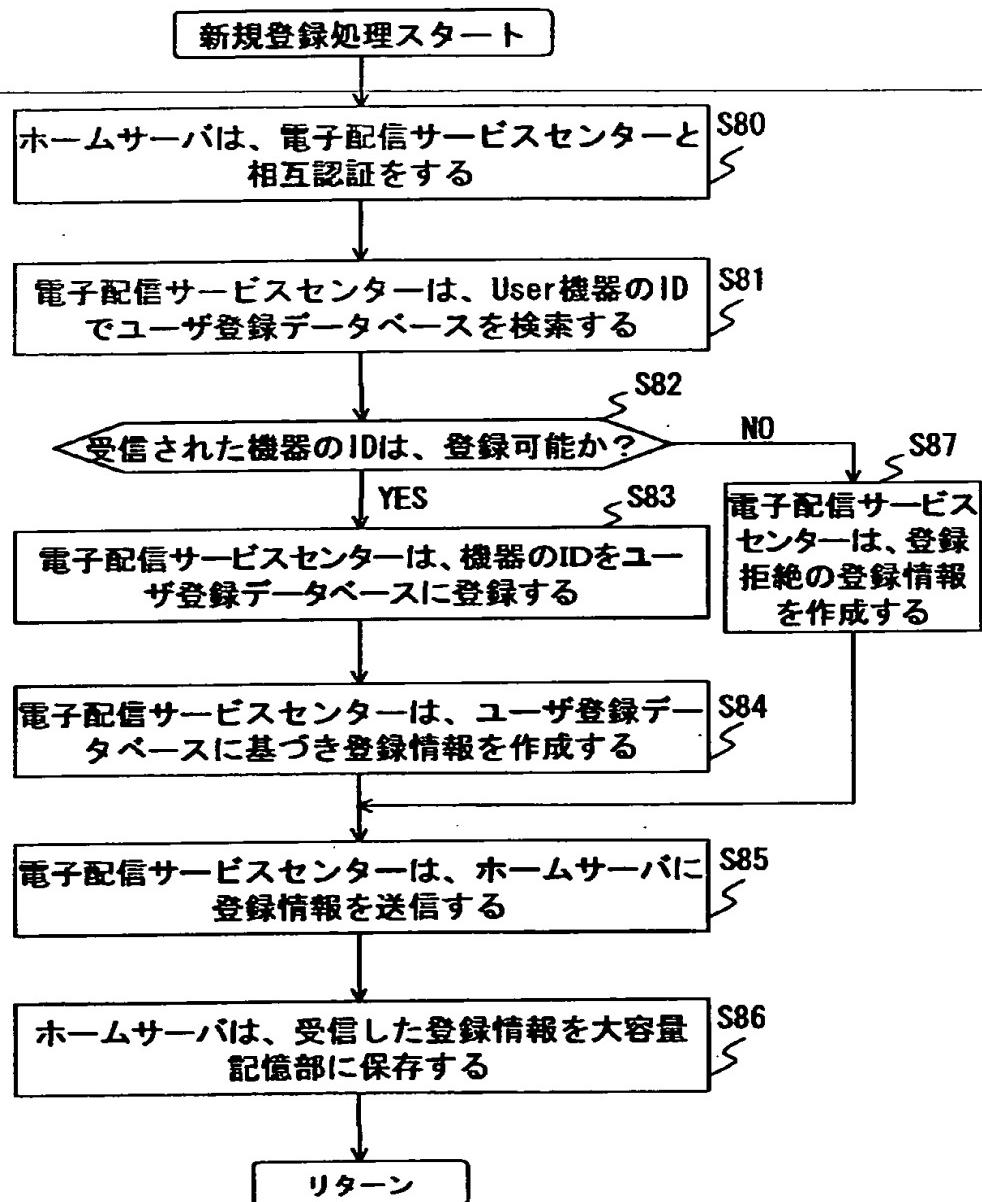


図59 機器IDの新規登録処理手順

【図64】

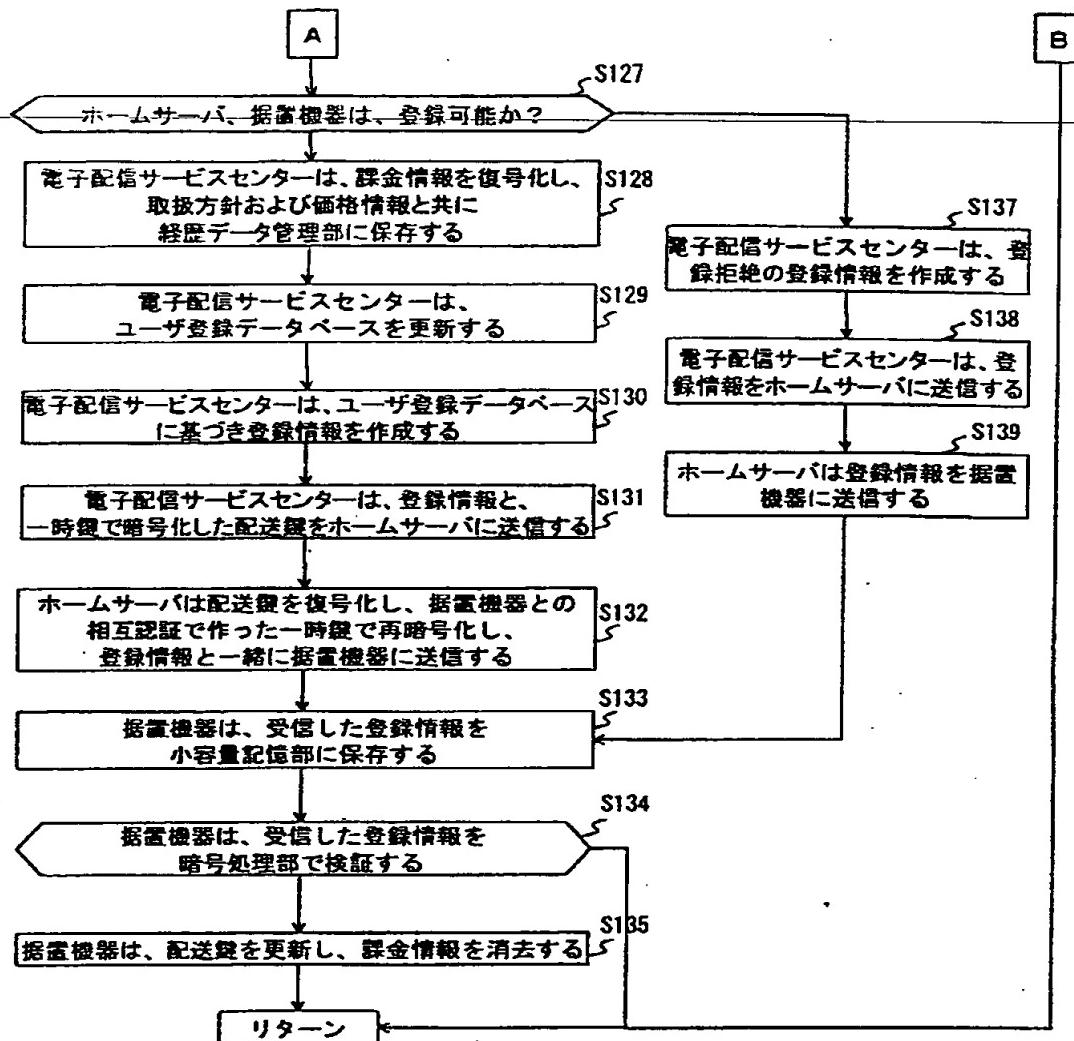


図64 据え置き機器による登録情報更新代理処理手順（2）

【図65】

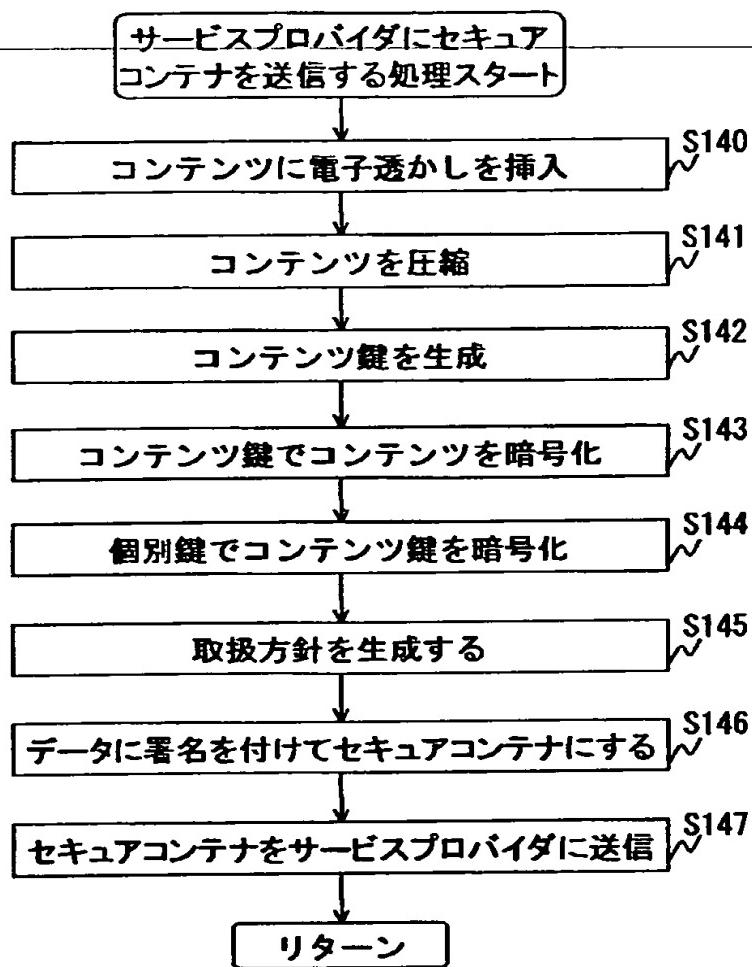


図65 セキュアコンテナの送信処理手順

【図66】

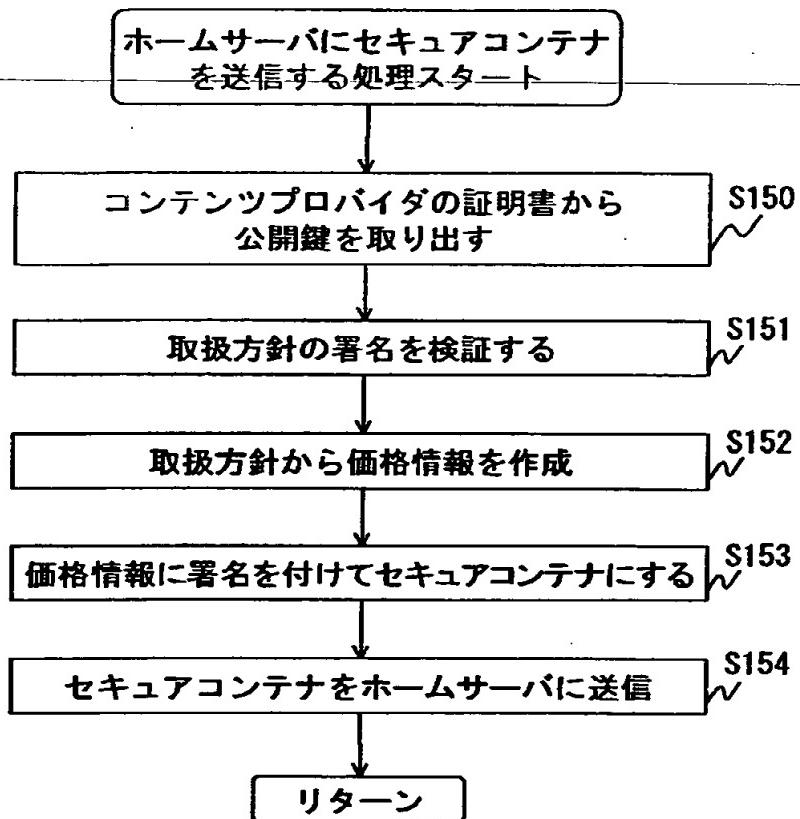


図66 セキュアコンテナの送信処理手順

【図67】

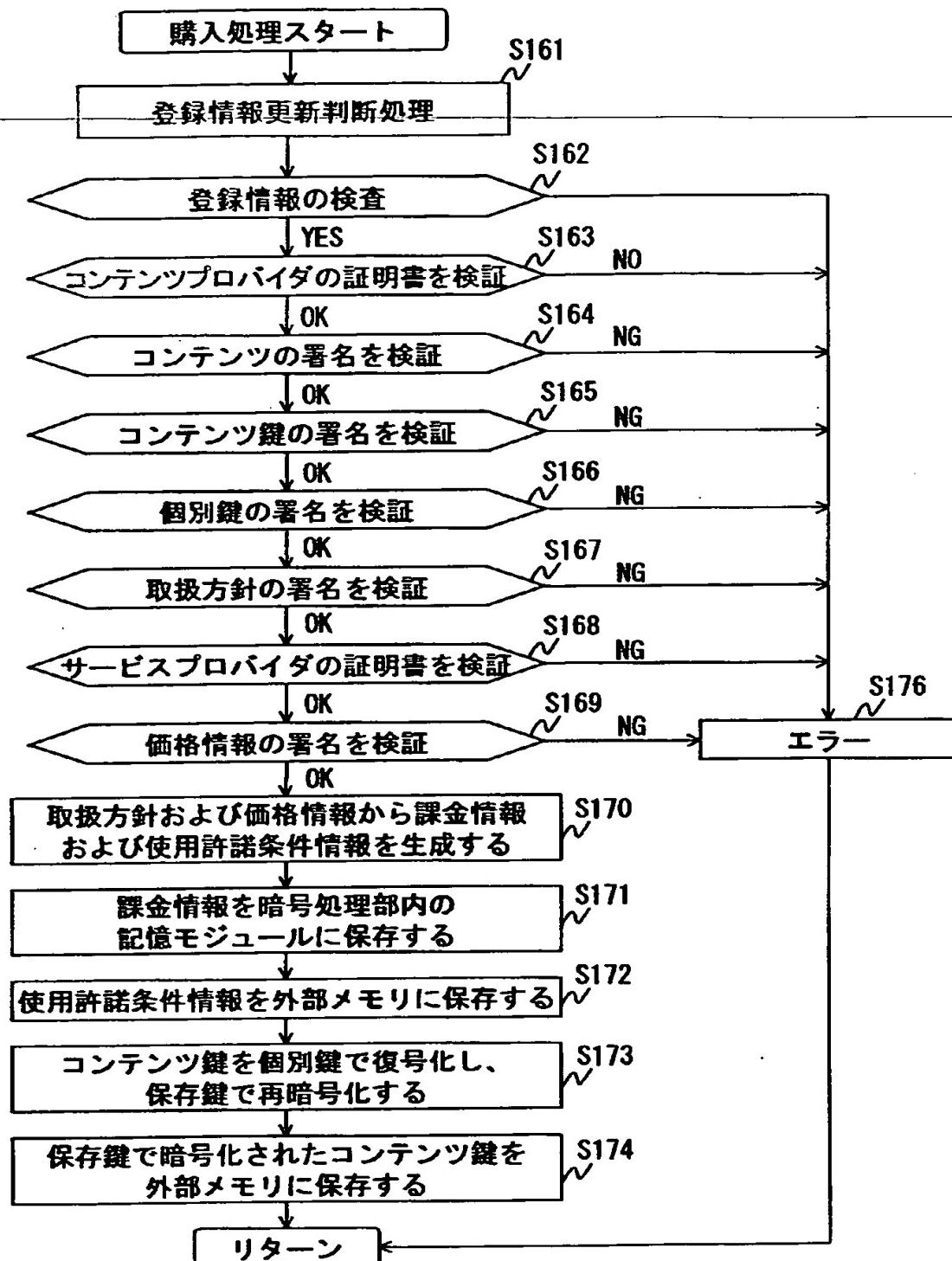


図67 ホームサーバの購入手順

【図68】

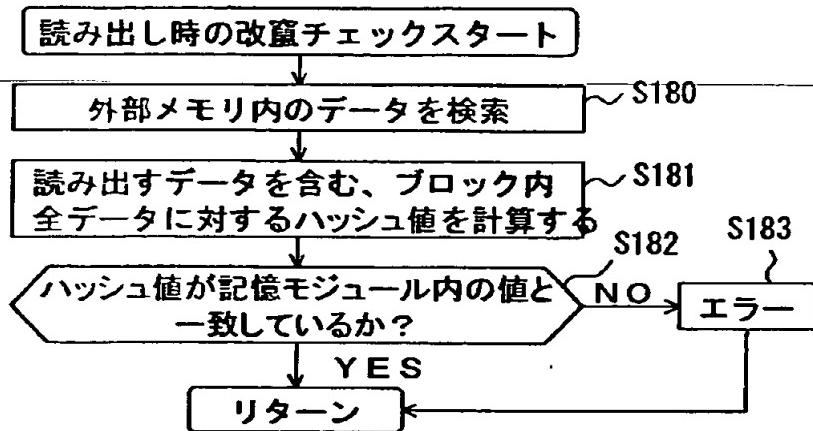


図68 データ読み出し時の改竄チェック処理手順

【図69】

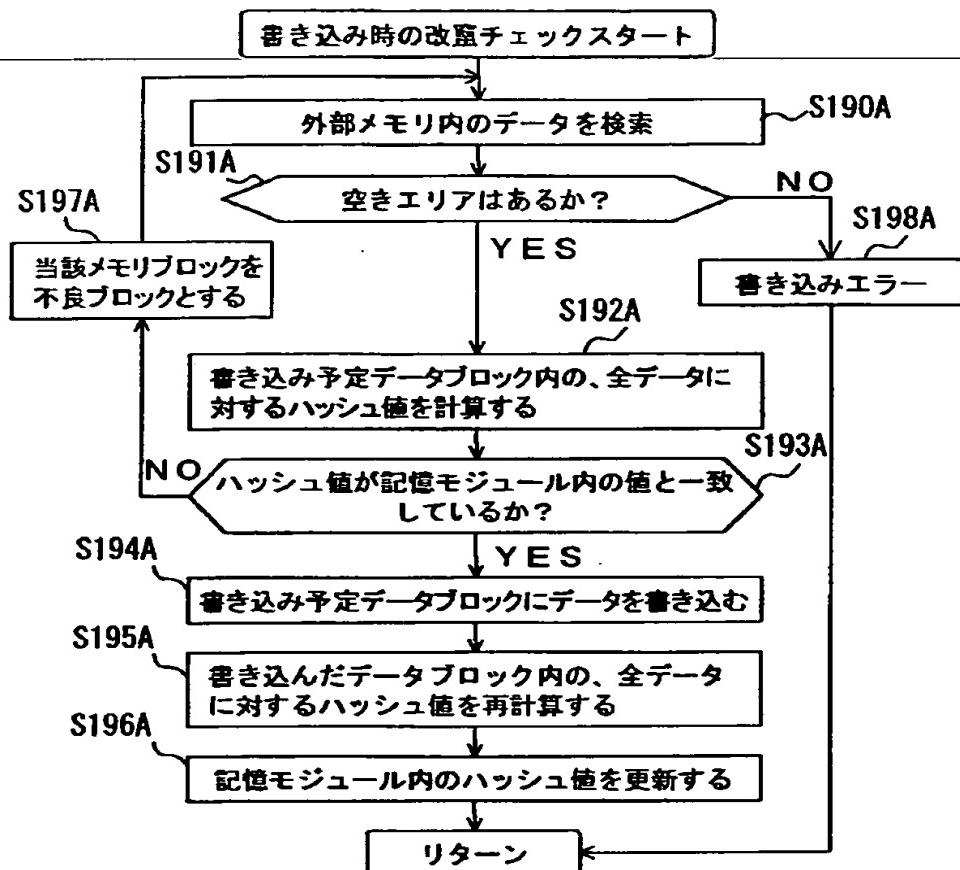


図69 データ書き込み時の改竄チェック処理手順

【図70】

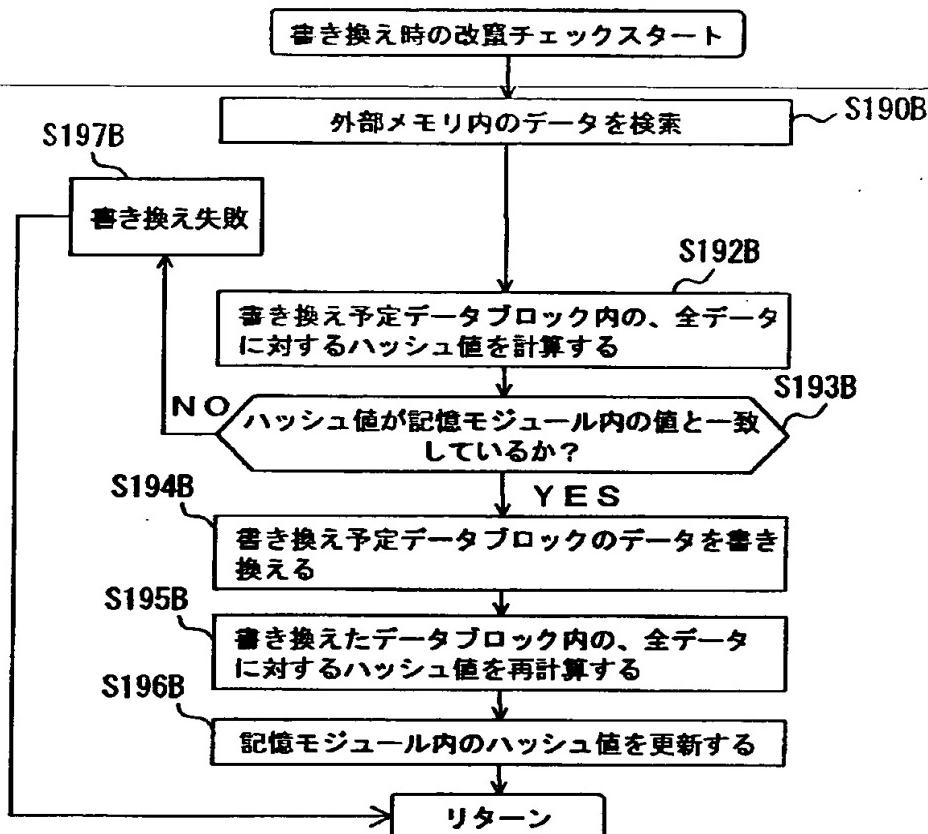


図70 データ書換え時の改竄チェック処理手順

【図71】

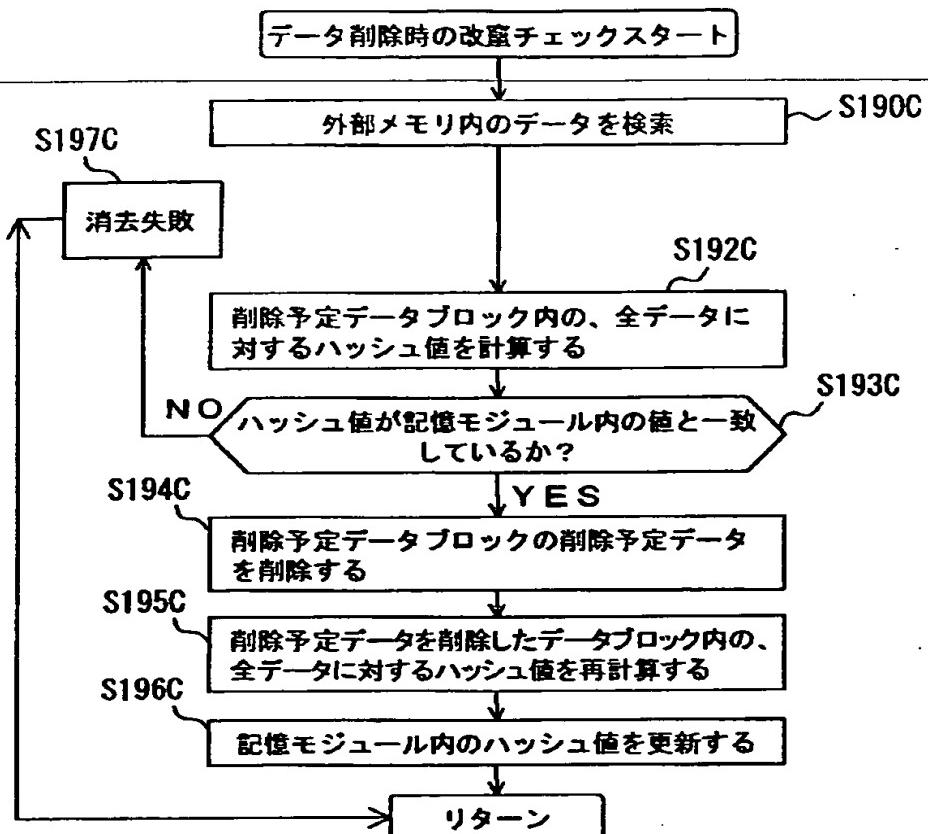


図71 データ削除時の改竄チェック処理手順

【図72】

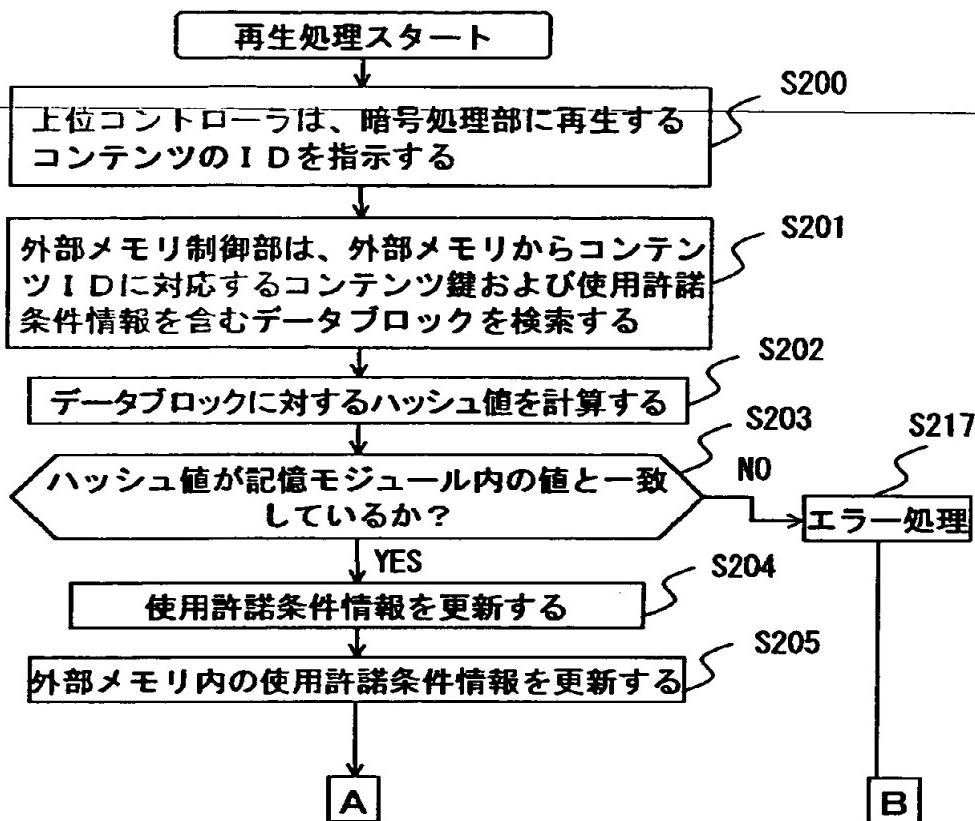


図72 ホームサーバによるコンテンツの再生処理手順（1）

【図73】

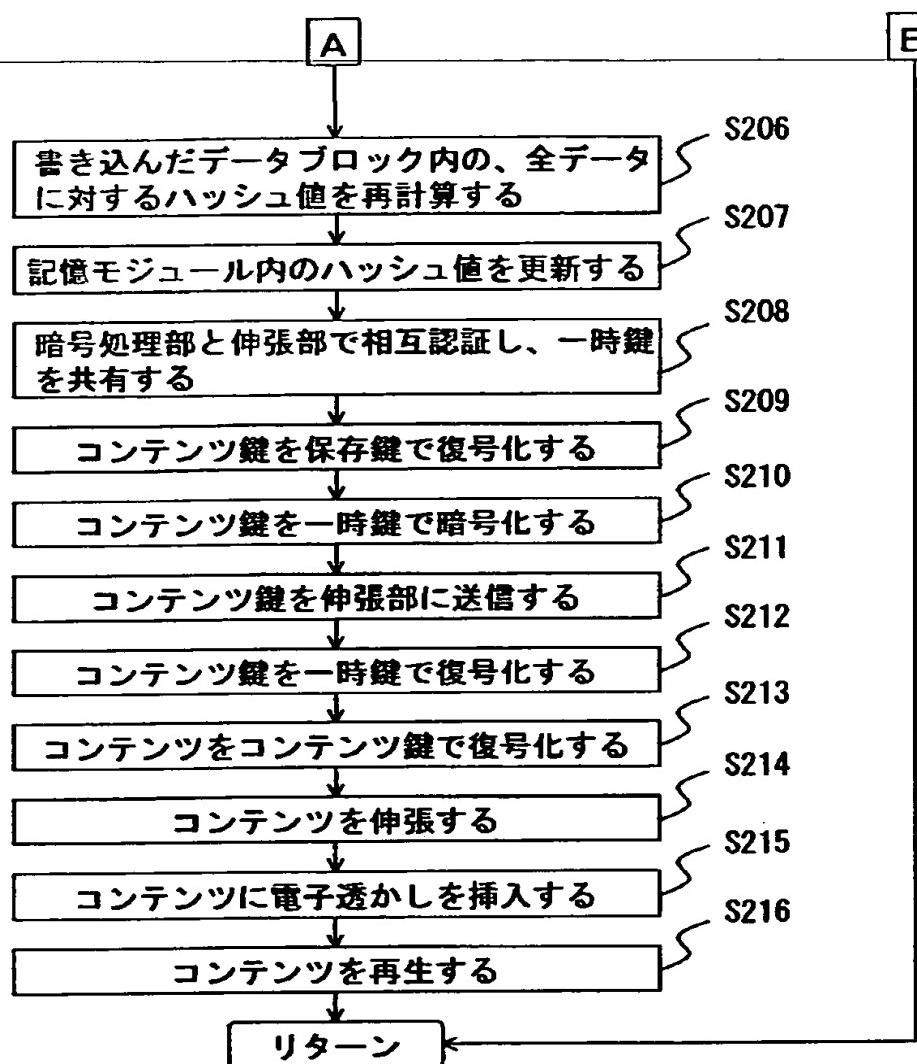


図73 ホームサーバによるコンテンツの再生処理手順（2）

【図74】

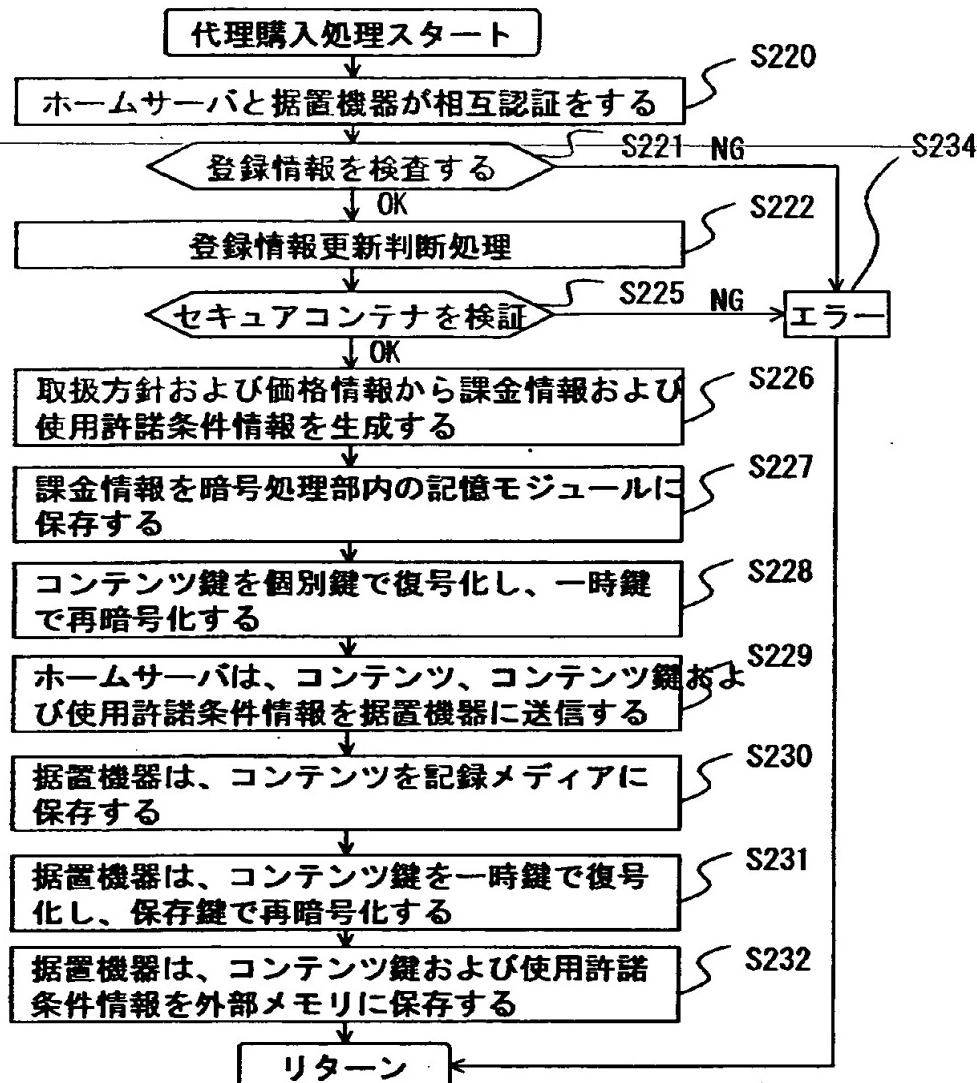


図74 ホームサーバによるコンテンツ利用権の代理購入処理手順

【図75】

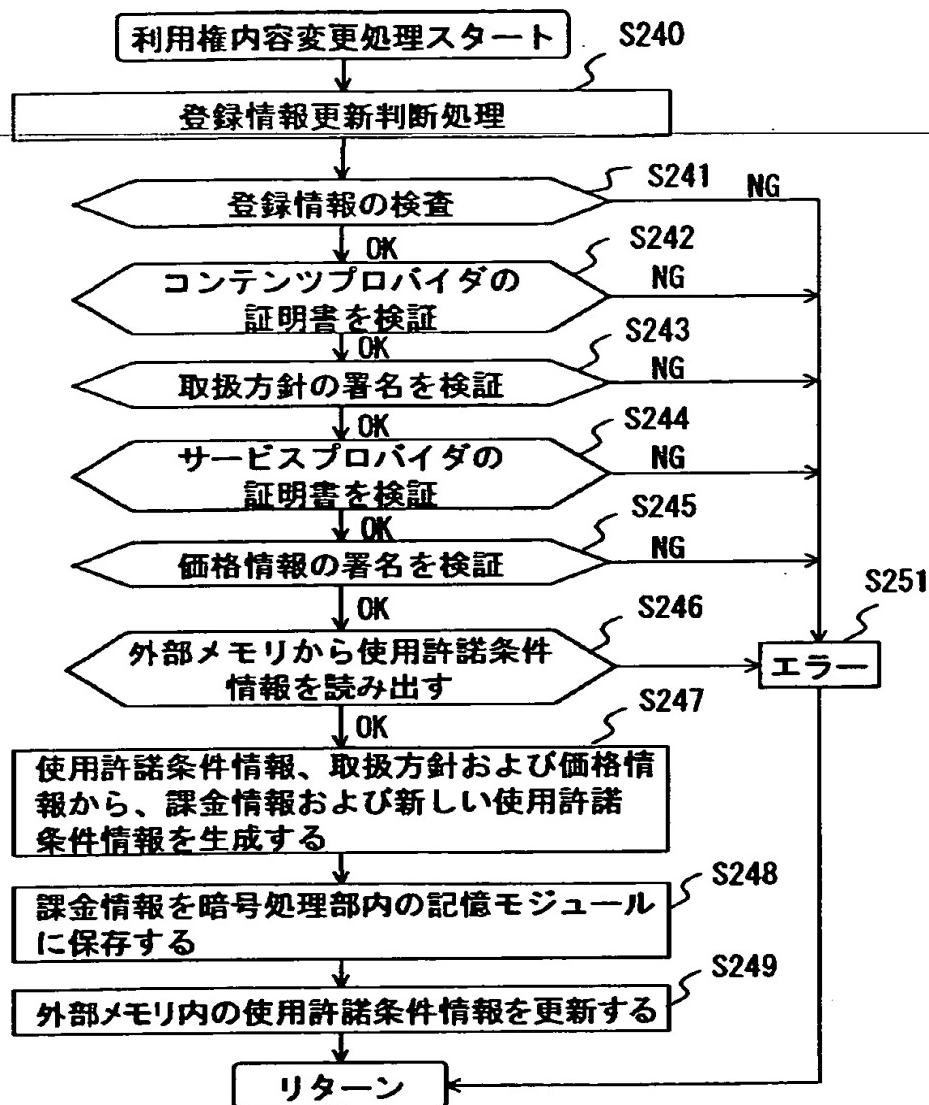


図75 購入済み利用者の内容変更処理手順

【図76】

ル ー ル n	ルール番号
	利用権内容番号
	パラメータ
	最低価格
	取り分(利益率)
ル ー ル 1	ルール番号#1
	利用権内容番号 #1
	なし
	¥350
	30%
ル ー ル 2	ルール番号#2
	利用権内容番号 #2
	1時間
	¥100
	30%
ル ー ル 3	ルール番号#3
	利用権内容番号 #6
	1回
	¥30
	30%
ル ー ル 4	ルール番号#4
	利用権内容番号 #13
	#2/#1
	¥200
	20%
ル ー ル 5	ルール番号#5
	利用権内容番号 #14
	#1/#1
	¥250
	20%

図76 取扱方針のルール部の一部

【図77】

ル ー ル n	ルール番号 パラメータ 価格
ル ー ル 1	ルール番号#1 30% ¥500
ル ー ル 2	ルール番号#2 40% ¥100
ル ー ル 3	ルール番号#3 40% ¥100
ル ー ル 4	ルール番号#4 10% ¥200
ル ー ル 5	ルール番号#5 20% ¥350

図77 価格情報のルール部の一部

【図78】

ルール1	#1
	#1
	なし
	¥350
	30%
ルール2	#2
	#2
	1時間
	¥100
	30%
ルール3	#3
	#13
	#2/#1
	¥200
	20%

取扱方針のルール部の一部

ルール1	#1
	30%
	¥500
ルール2	#2
	40%
	¥100
ルール3	#3
	10%
	¥200

価格情報のルール部の一部

現在

ルール	ルール番号
	利用権内容番号
	パラメータ
ルール	#2
	#2
	30分／2時間

使用許諾条件情報のルール部

変更後

ルール	ルール番号
	利用権内容番号
	パラメータ
ルール	#1
	#1
	なし

使用許諾条件情報のルール部

図78 権利内容の変更例

【図79】

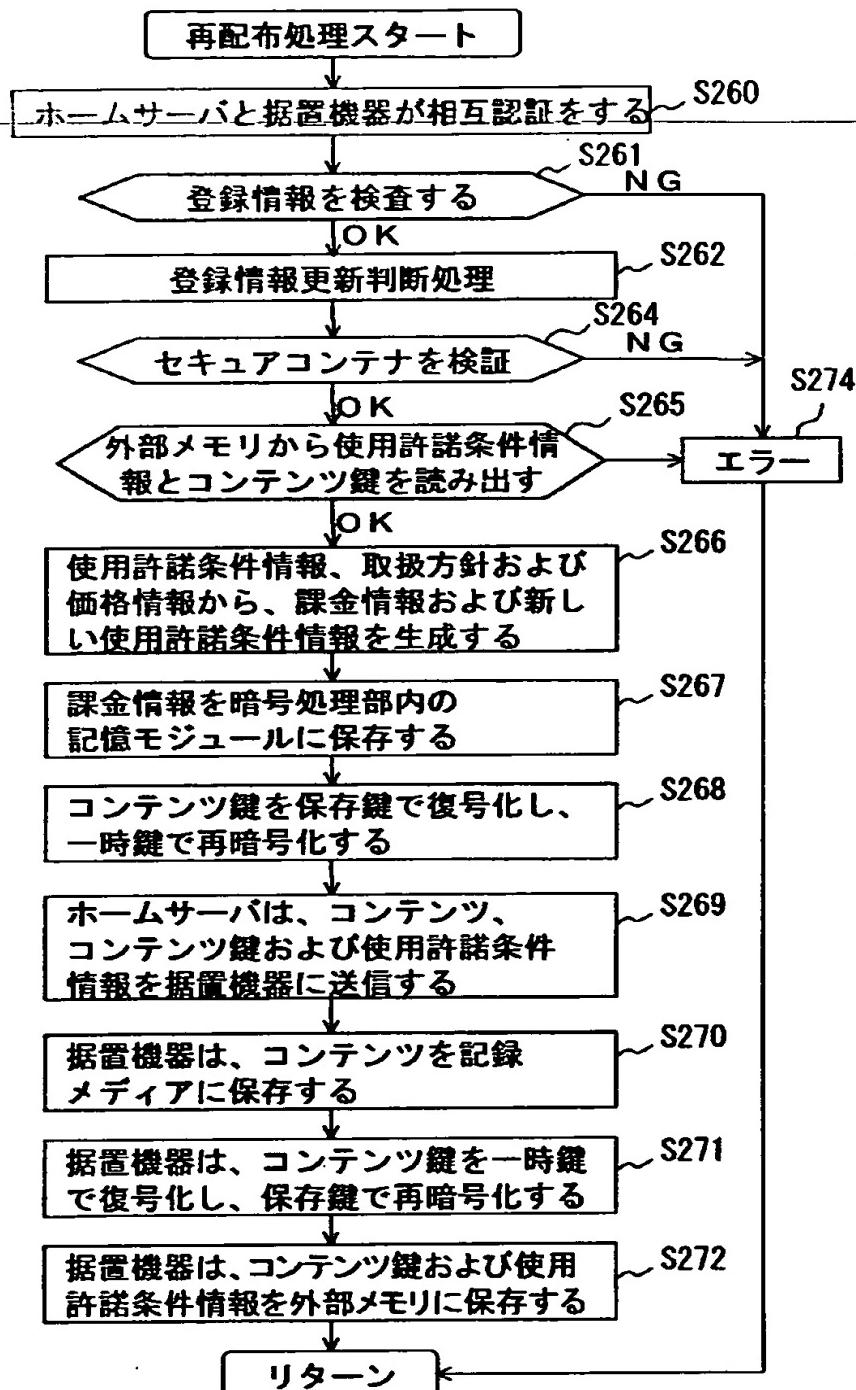


図79 コンテンツ利用権の再配布処理手順

【図80】

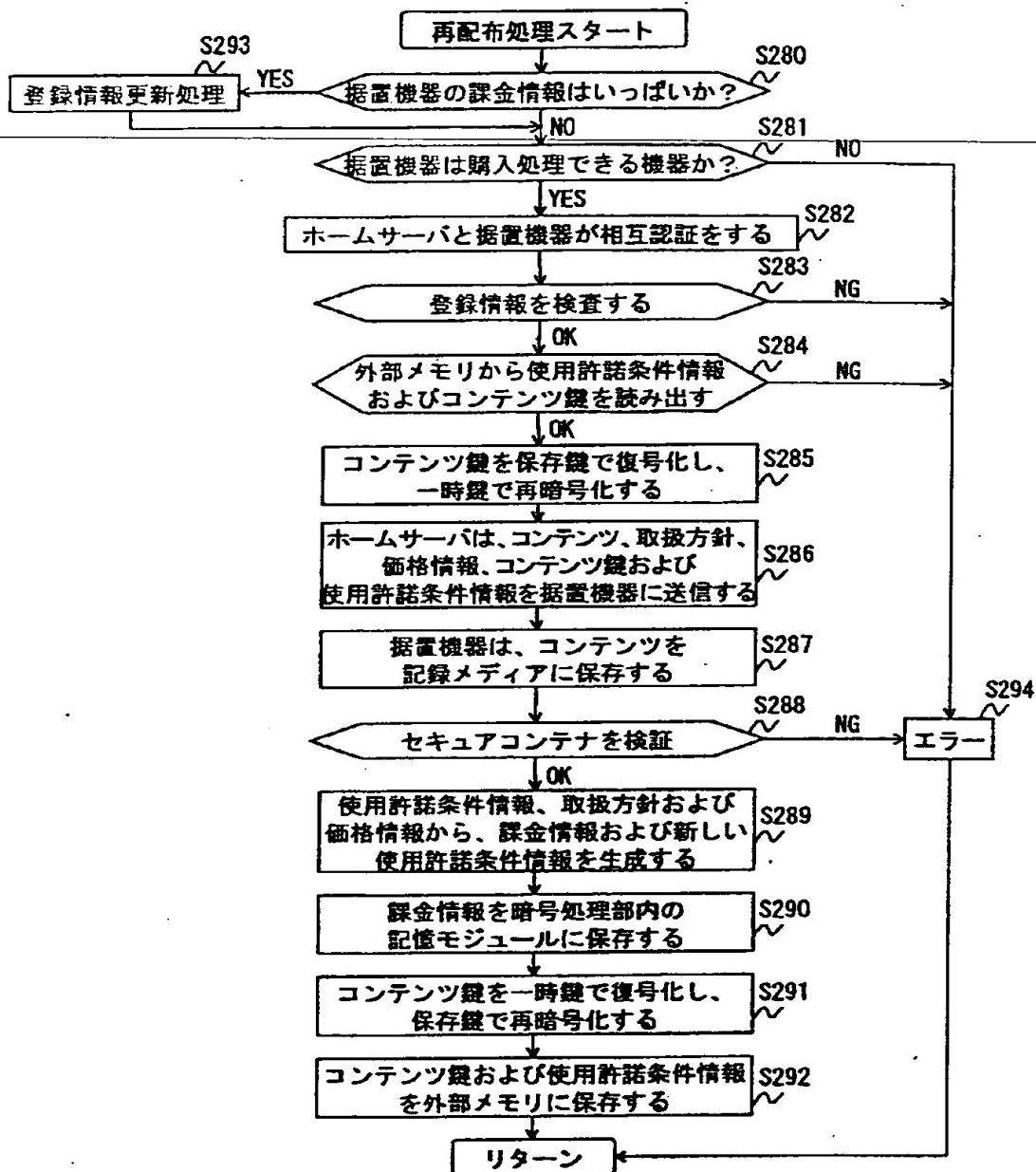


図80 据置機器でのコンテンツ利用権購入処理手順

【図81】

ルール 1	ルール番号 #1
	利用権内容番号 #1
	なし
	¥350
	30%
ルール 2	ルール番号 #2
	利用権内容番号 #16
	なし
	¥100
	50%
ルール 1	ルール番号 #1
	30%
	¥500
	ルール番号 #2
	0%
ルール 2	¥100

取扱方針のルール部の一部

価格情報のルール部の一部

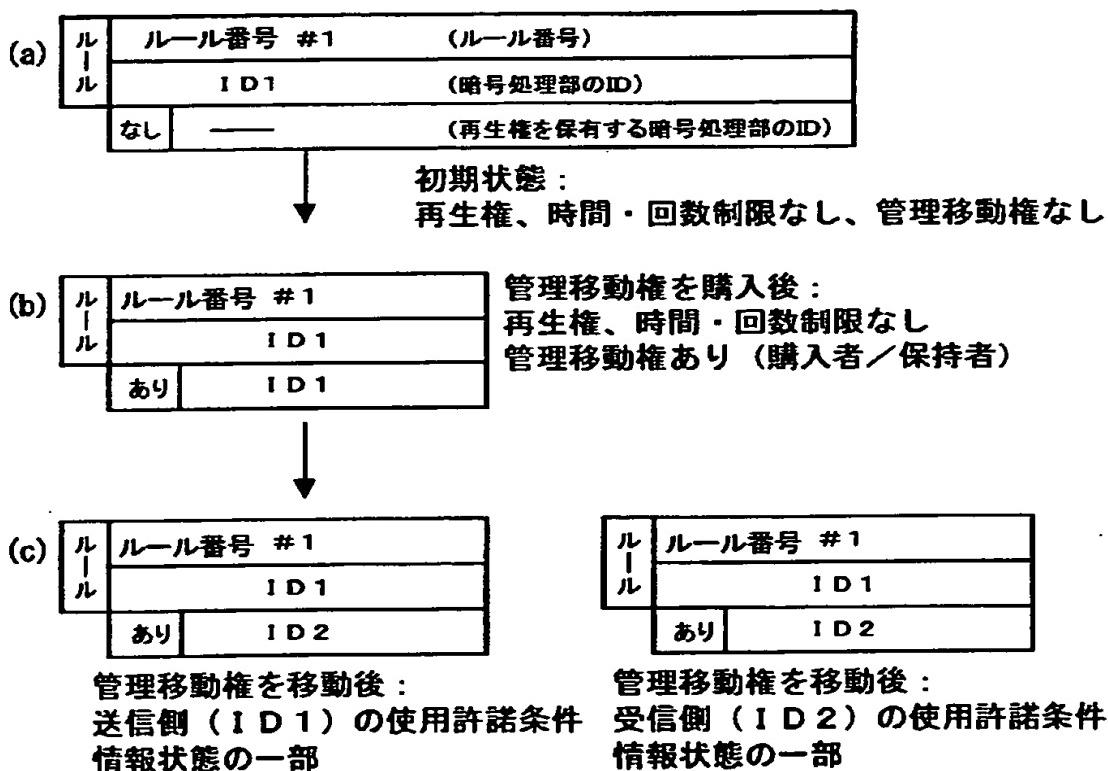


図81 使用許諾条件情報のルール部の変遷

【図82】

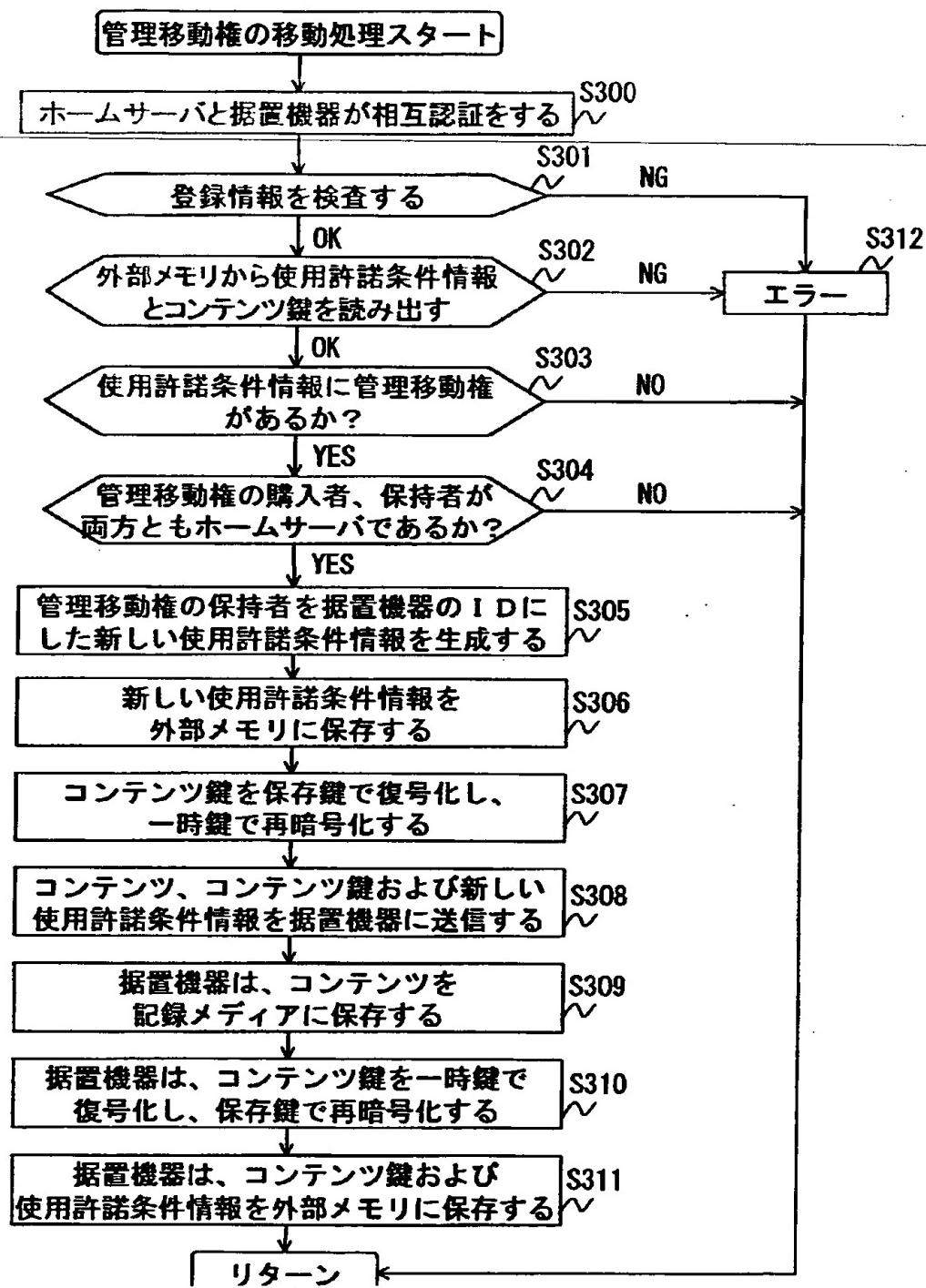


図82 管理移動権の移動処理手順

【図 8 3】

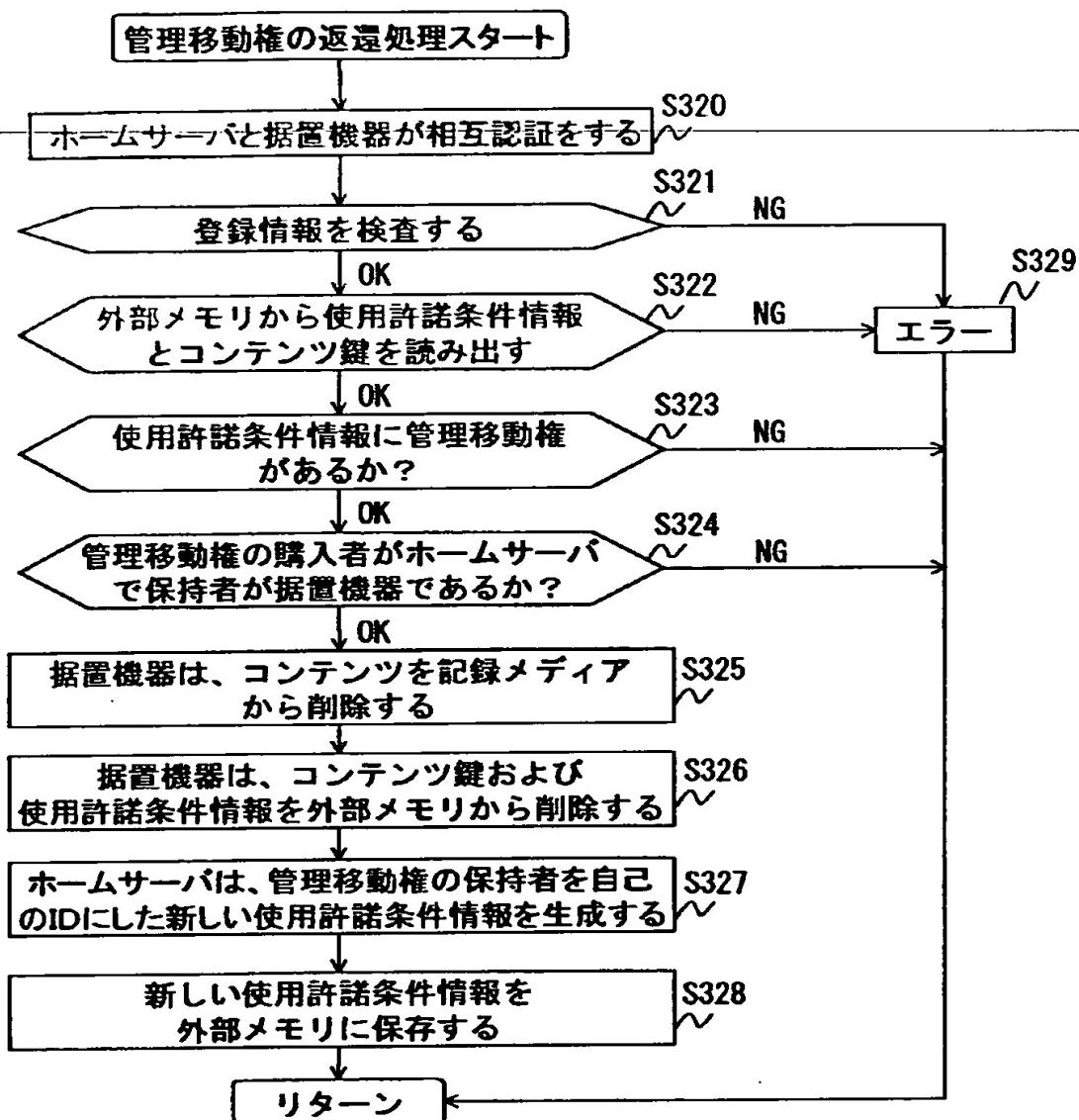


図 8 3 管理移動権の返還処理手順

【図84】

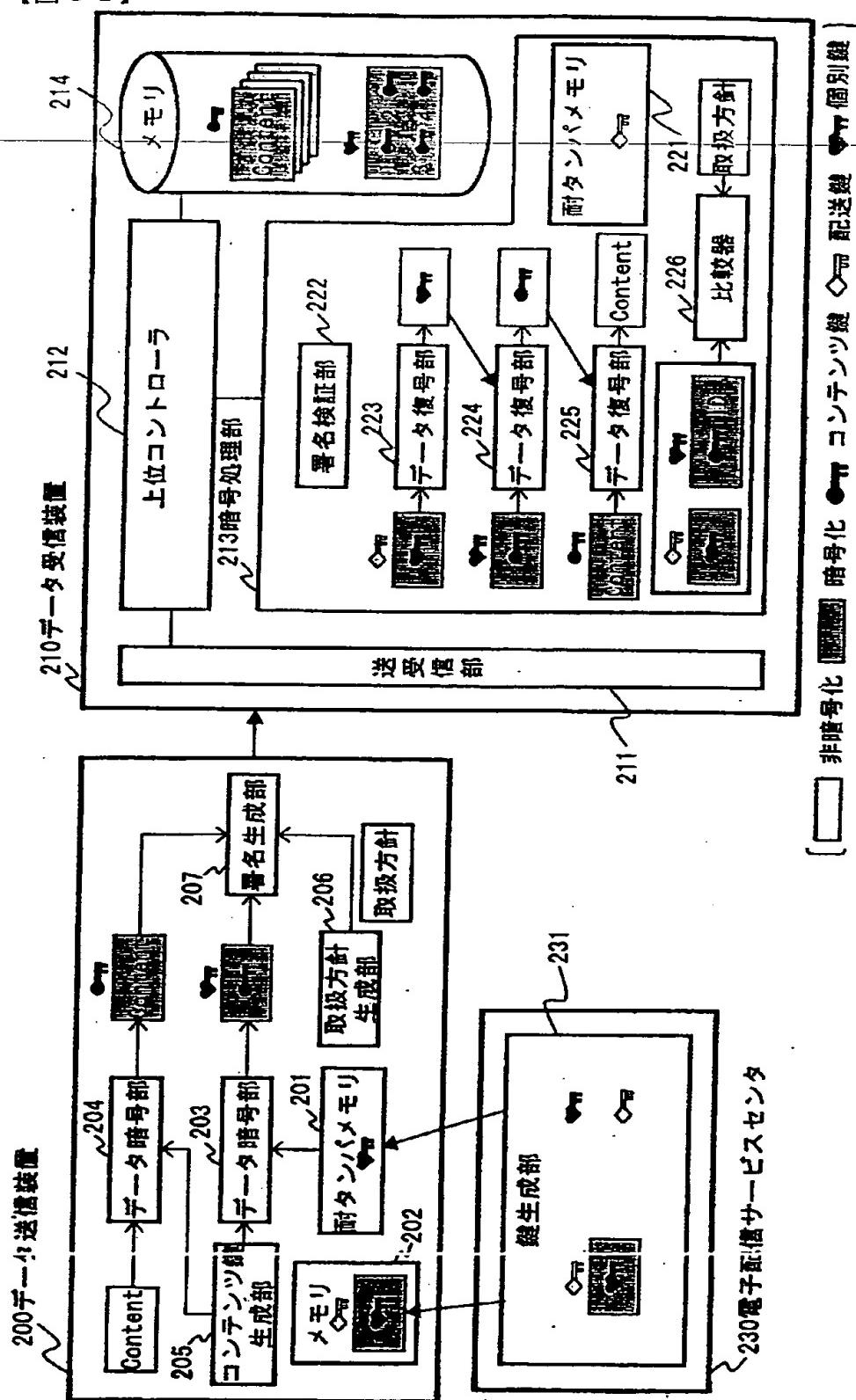


図84 情報送信システム(1)

【図85】

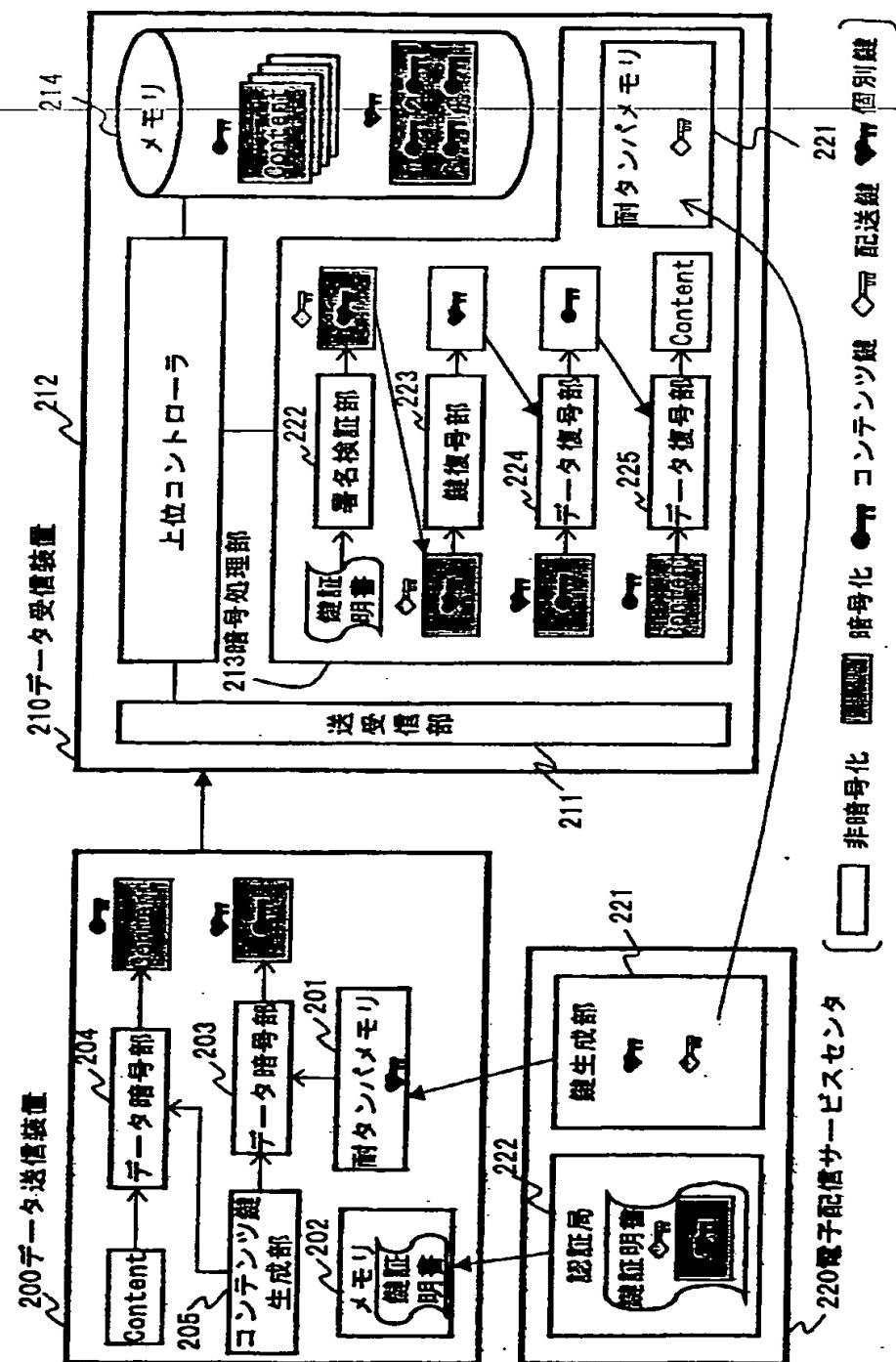


図85 情報送信システム(2)

【図86】

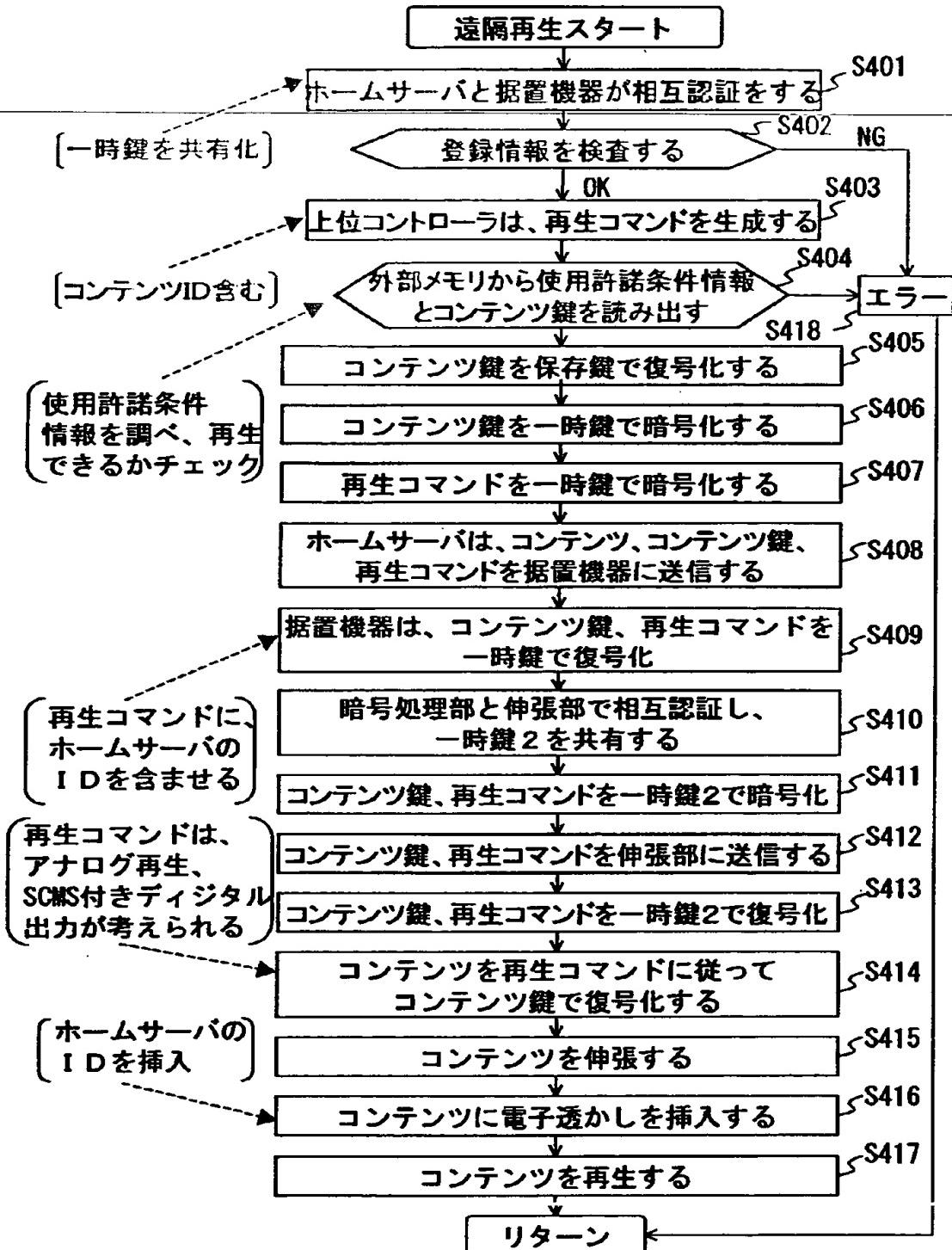


図86 遠隔再生処理手順

【図87】

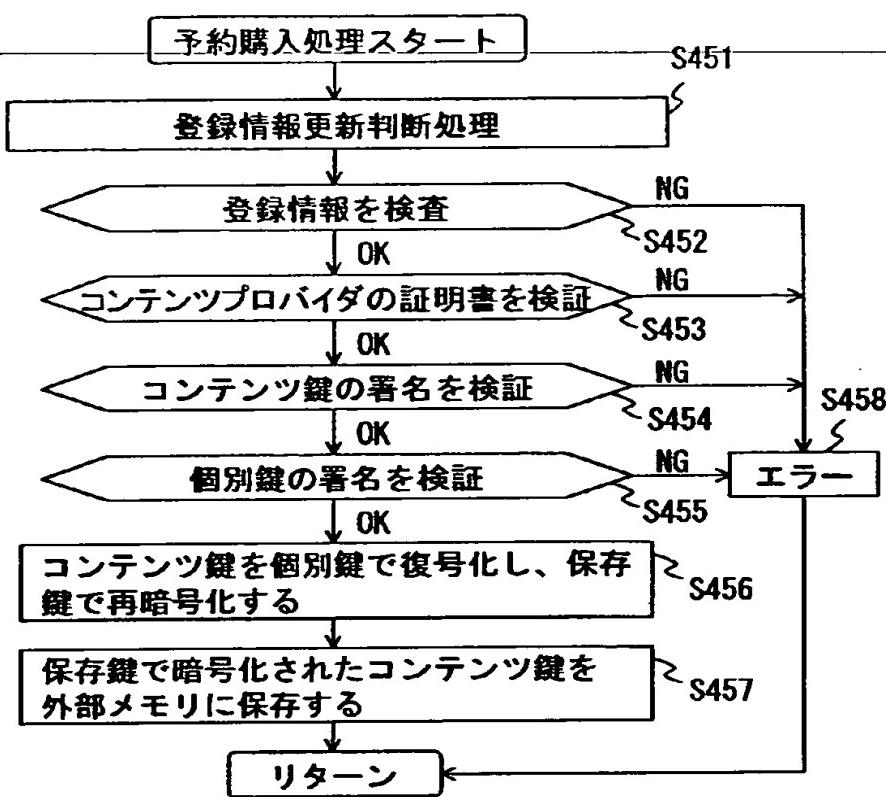


図87 予約購入処理手順

【図88】

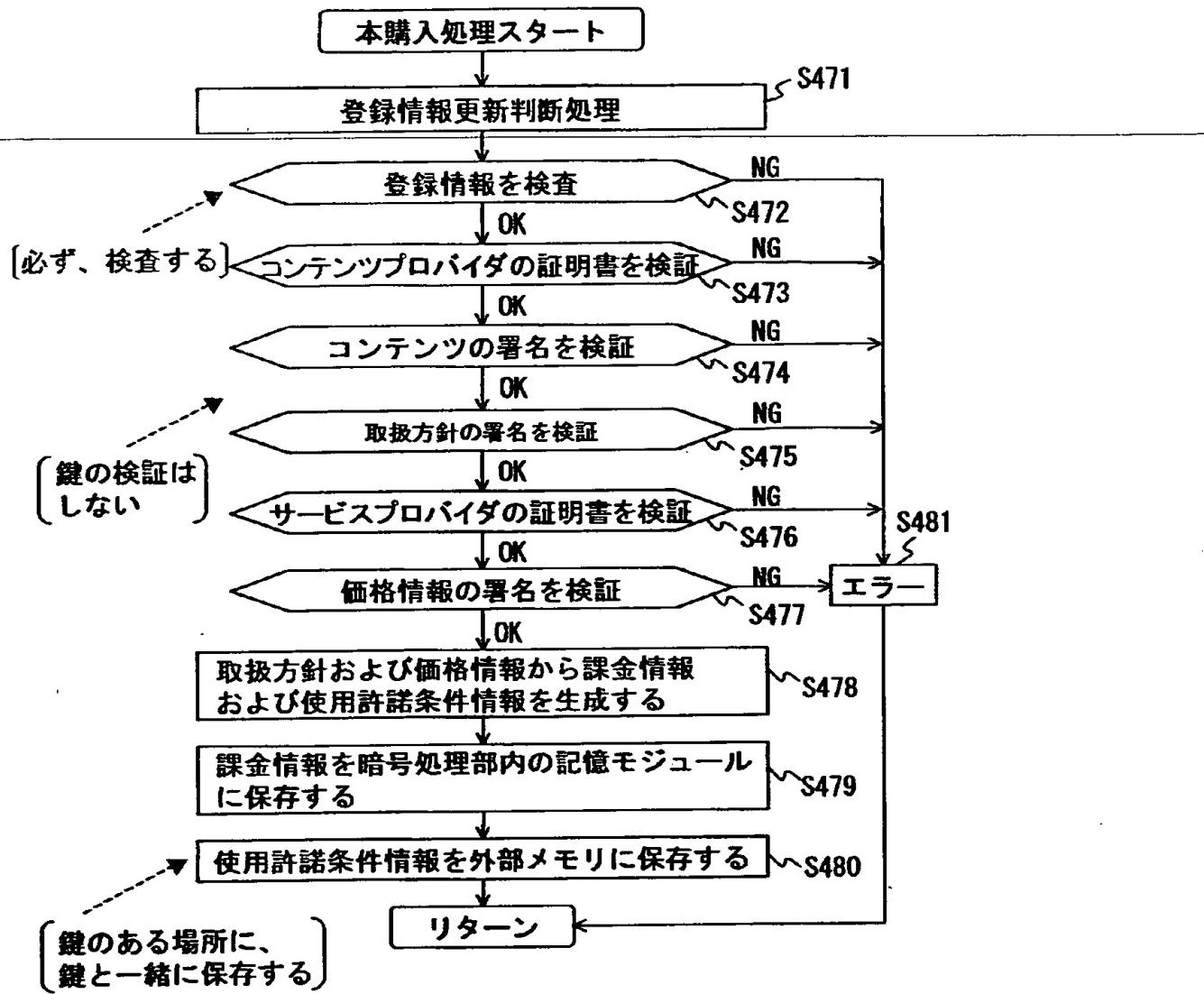


図88 予約購入後の本購入処理手順

【図89】

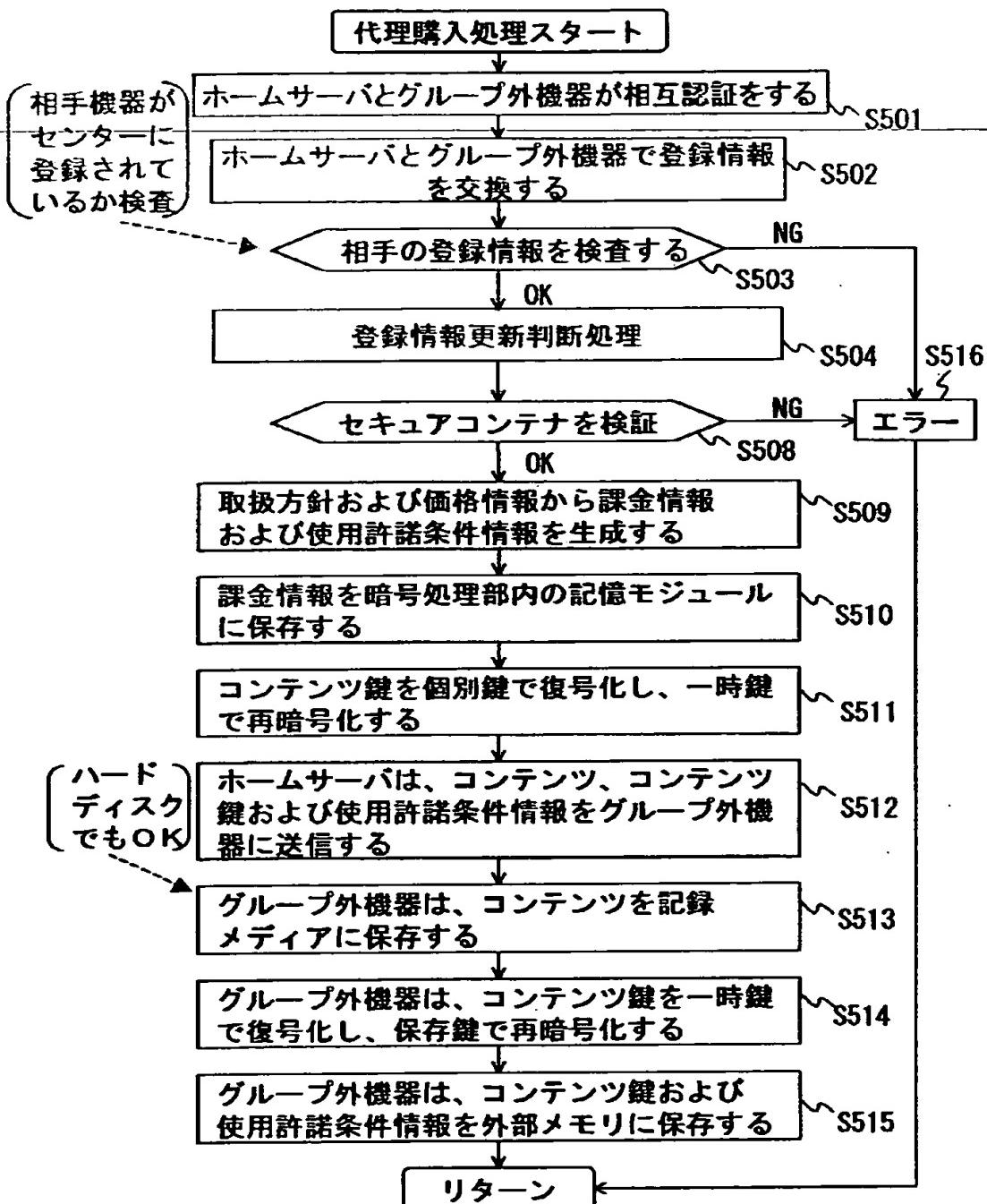


図89 代理購入処理手順（ホームサーバが支払う場合）

【図90】

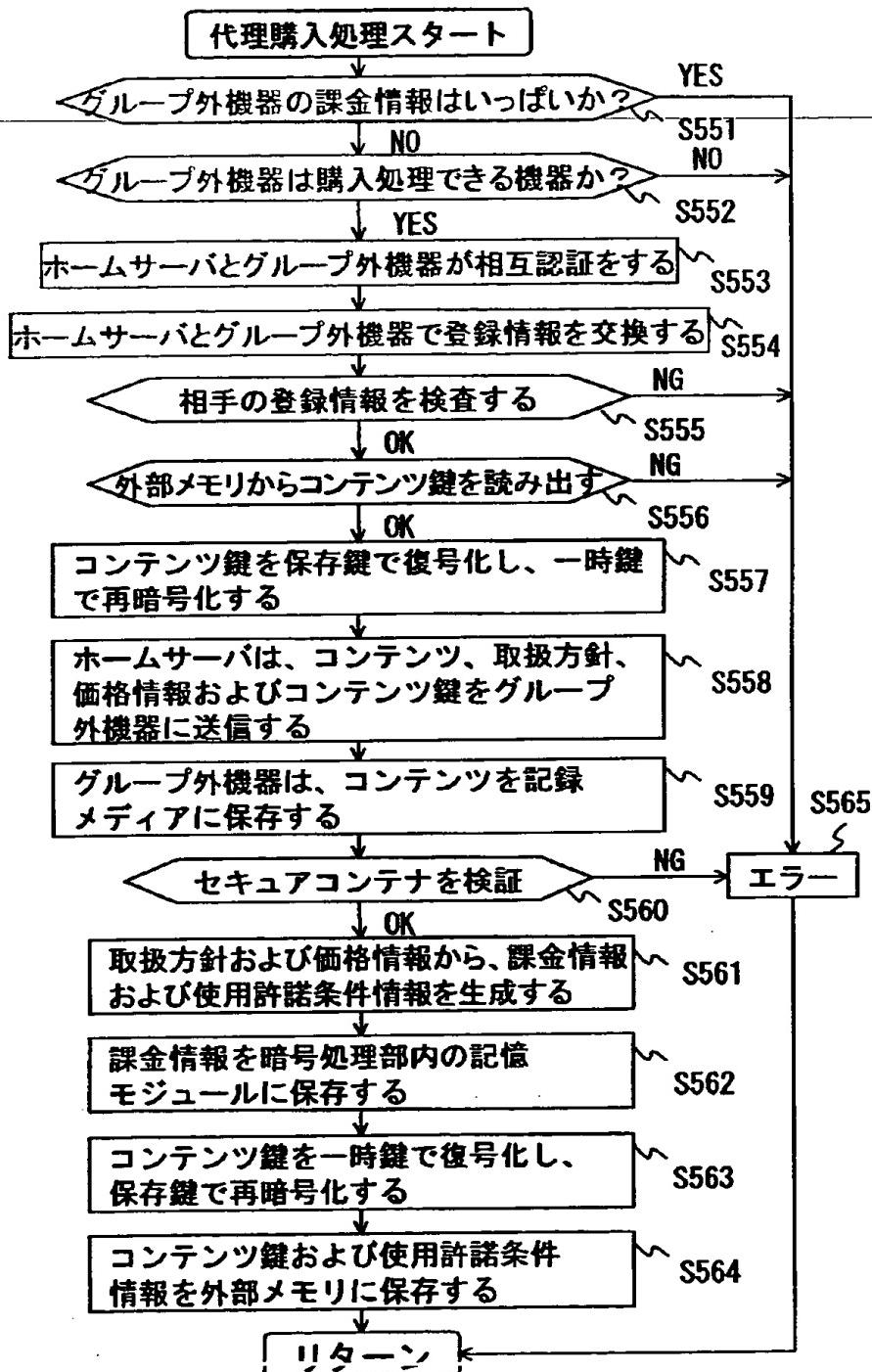


図90 代理購入処理手順（グループ外機器が支払う場合）

【図91】

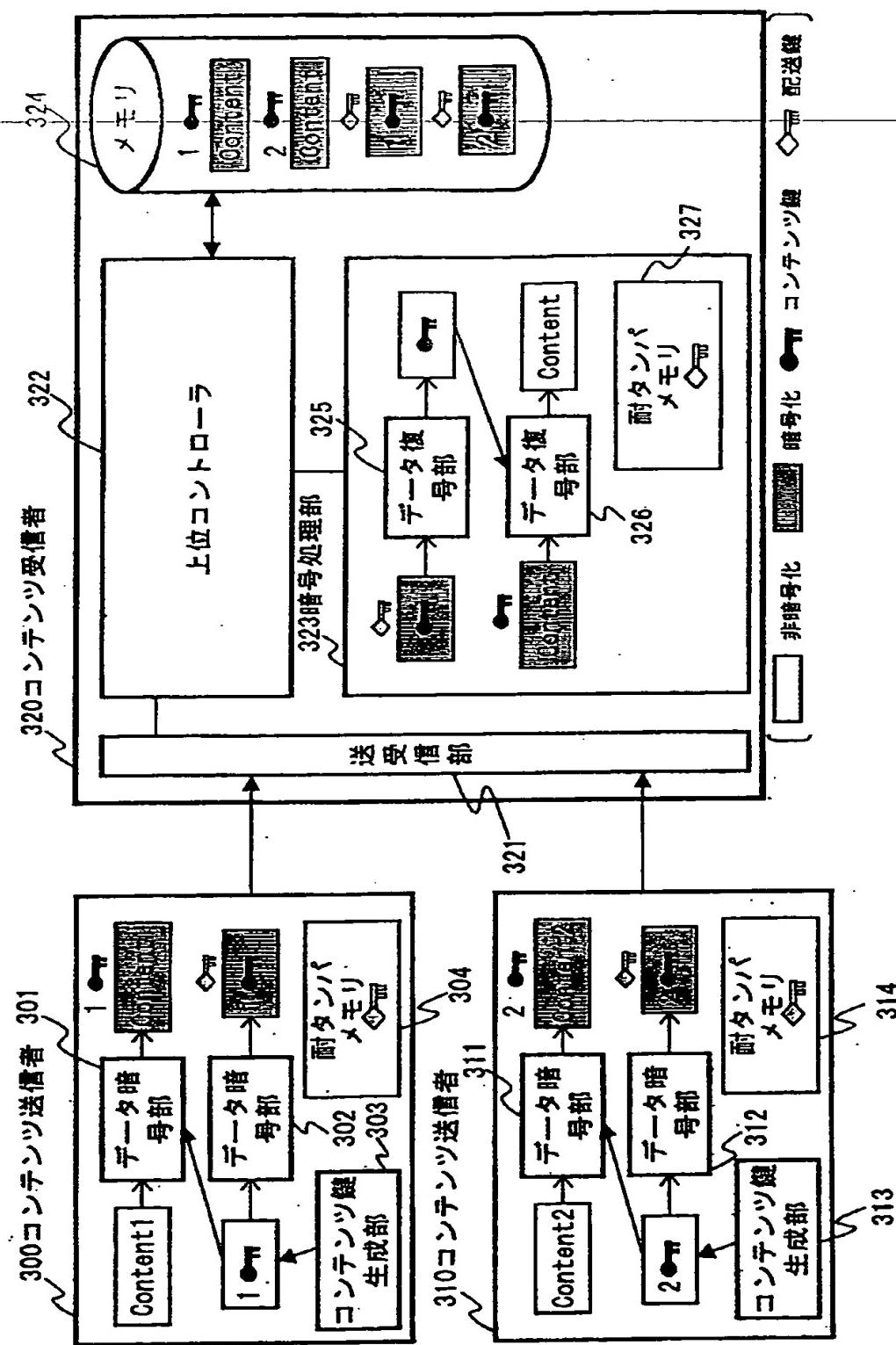


図91 従来例

【書類名】 要約書

【要約】

【課題】

コンテンツを配信する情報配信システムにおいて、コンテンツを利用する情報受信装置のうち、コンテンツの利用権を有していない情報受信装置でもコンテンツを利用できるようにする。

【解決手段】

コンテンツの利用権を有する情報受信装置は、情報送信装置から配信されるコンテンツデータを復号するためのコンテンツ鍵を有し、コンテンツデータの利用権を持たない他の機器に対する再生コマンドを生成し、当該生成された再生コマンド及びコンテンツ鍵を他の機器に送信することにより、他の機器は受け取った再生コマンド及びコンテンツ鍵を用いてコンテンツを再生することができる。

【選択図】 図85

出願人履歴情報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社

This Page Blank (uspto)